About the command references

The command references describe the commands and command syntax options available for the following switch series:

- S5120V2-LI.
- S3100V3-SI.
- S5110V2.
- S5110V2-SI.
- S5000V3-EI.
- S5000V5-EI.
- S5000E-X.
- S5000X-EI.
- S5130S-LI.
- S5120V3-LI.
- S5120V3-SI.
- MS4320V2.
- MS4320V3.
- MS4320.
- MS4300V2.
- MS4200.
- WS5810-WiNet.
- WS5820-WiNet.
- WAS6000.

Command reference	Content
Fundamentals Command Reference	Covers the commands for logging in to and setting up the device. This command reference includes: • CLI (command privilege settings and CLI management commands). • RBAC. • Logging in to the switch. • FTP and TFTP. • File system management. • Configuration file management. • Software upgrade. • Device management. • Tcl. • Python. • License management.
Virtual Technologies Command Reference	Covers the commands for configuring the Intelligent Resilient Framework (IRF) technology features. It covers planning the switch roles in the IRF fabric, connecting the IRF links, and detecting and maintaining the IRF fabric.
Layer 2—LAN Switching Command Reference	Covers the commands for configuring Layer 2 technologies and features in a LAN switched network. This command reference includes:

Command reference	Content
	• Ethernet interface. • Loopback, null, and inloopback interfaces. • Bulk interface configuration. • MAC address table and MAC Information. • Ethernet link aggregation. • Port isolation. • Spanning tree. • Loop detection. • VLAN (including VLAN, private VLAN, and voice VLAN). • MVRP. • QinQ. • VLAN mapping. • LLDP. • L2PT. • PPPoE relay.
Layer 3—IP Services Command Reference	Covers the commands for configuring and managing IP addressing (including static and dynamic IPv4 and IPv6 address assignment), network performance optimization, and ARP. This command reference includes: • ARP (including gratuitous ARP, proxy ARP, ARP snooping, and ARP direct route advertisement). • IP addressing. • DHCP. • DNS. • Basic IP forwarding. • Fast forwarding. • IP performance optimization. • UDP helper. • IPv6 basics. • DHCPv6. • IPv6 fast forwarding. • HTTP redirect.
Layer 3—IP Routing Command Reference	Covers the commands for configuring routes for IPv4 and IPv6 networks of different sizes, route filtering, route control, and policy-based routing. This command reference includes: • Basic IP routing. • Static routing. • RIP. • OSPF. • Policy-based routing. • IPv6 static routing. • RIPng. • OSPFv3. • IPv6 policy-based routing. • Routing policy.
IP Multicast Command Reference	Covers the commands for Layer 2 IPv4 multicast protocols (including IGMP snooping, PIM snooping, and multicast VLAN) and Layer 2 IPv6 multicast protocols (including MLD snooping, IPv6 PIM snooping, and IPv6 multicast VLAN). This command reference includes: • IGMP snooping.

Command reference	Content
	• PIM snooping. • Multicast VLAN. • MLD snooping. • IPv6 PIM snooping. • IPv6 multicast VLAN.
ACL and QoS Command Reference	Covers the commands for classifying traffic with ACLs, and allocating network resources and managing congestions with QoS technologies to improve network performance and network use efficiency. This command reference includes: • ACL. • QoS (including QoS policy, priority mapping, GTS and rate limit, congestion management, and aggregate CAR). • Data buffer. • Time range.
Security Command Reference	Covers security feature commands. Available security features include identity authentication (AAA), access security (802.1X, MAC authentication, and port security), secure management (SSH), SSL, and attack protection (IP source guard and ARP attack protection). This command reference includes: • AAA. • 802.1X. • MAC authentication. • Portal. • Web authentication. • Port security. • User profile. • Password control. • Public key management. • PKI. • IPsec (including IPsec, IKE, and IKEv2). • SSH. • SSL. • Attack detection and prevention. • TCP attack prevention. • IP source guard. • ARP attack protection. • ND attack defense. • SAVI. • MFF. • Crypto engine. • FIPS. • 802.1X client.
High Availability Command Reference	Covers high availability commands for managing failure detection and failover. Failure detection technologies focus on fault detection and isolation. Failover technologies focus on network recovery. This command reference includes: • Ethernet OAM. • CFD. • DLDP. • RRPP. • ERPS.

Command reference	Content
	• Smart Link. • Monitor Link. • VRRP. • BFD. • Track. • Loopback MAC SWAP.
Network Management and Monitoring Command Reference	Covers the commands that help you manage and monitor your network, for example, manage system events, collect traffic statistics, sample packets, assess network performance, and test network connectivity. This command reference includes: • System maintenance and debugging (ping, tracert, and system debugging). • NQA. • NTP and SNTP. • PoE. • SNMP. • RMON. • NETCONF. • CWMP. • EAA. • Process monitoring and maintenance. • Mirroring (including both port and traffic mirroring). • sFlow. • Information center. • VCF fabric. • Cloud connection. • SmartMC. • WiNet.
Telemetry Command Reference	Covers the commands for configuring gRPC.
OpenFlow Command Reference	Covers the commands for configuring OpenFlow.

Fundamentals Command Reference

This command reference is applicable to the following switches and software versions:

H3C S5120V2-LI switch series (Release 6308P01 and later)
H3C S3100V3-SI switch series (Release 6309P01 and later)
H3C S5110V2 switch series (Release 6310 and later)
H3C S5110V2-SI switch series (Release 6310 and later)
H3C S5000V3-EI switch series (Release 6310 and later)
H3C S5000V5-EI switch series (Release 6319P01 and later)
H3C S5000E-X switch series (Release 6310 and later)
H3C S5130S-LI switch series (Release 6310 and later)
H3C MS4320V2 switch series (Release 6308P01 and later)
H3C MS4320 switch series (Release 6308P01 and later)
H3C MS4300V2 switch series (Release 6308P01 and later)
H3C MS4200 switch series (Release 6310 and later)
H3C WS5810-WiNet switch series (Release 6308P01 and later)
H3C WS5820-WiNet switch series (Release 6308P01 and later)
H3C WAS6000 switch series (Release 6308P01 and later)
H3C S5000X-EI switch series (Release 6329 and later)
H3C MS4320V3 switch series (Release 6329 and later)
H3C S5120V3-SI switch series (Release 6329 and later)
H3C S5120V3-LI switch series (Release 6329 and later)

New H3C Technologies Co., Ltd.
http://www.h3c.com

Software version: Release 63xx
Document version: 6W105-20230524

Preface

This command reference describes commands that help you get started with the device. It includes the commands for the following features and tasks:

This preface includes the following topics about the documentation:

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Documentation feedback

You can e-mail your comments about product documentation to info@h3c.com.

We appreciate your comments.

Contents

Basic CLI commands

alias

Use **alias** to configure a command alias.

Use **undo alias** to delete a command alias.

Syntax

alias *alias command*

undo alias *alias*

Default

The device has a set of system-defined command aliases, as listed in Table 1.

Table 1 System-defined command aliases

Command alias	Command or command keyword
access-list	**acl**
end	**return**
erase	**delete**
exit	**quit**
hostname	**sysname**
logging	**info-center**
no	**undo**
show	**display**
write	**save**

Views

System view

Predefined user roles

network-admin

Parameters

alias: Specifies an alias, a case-sensitive string of 1 to 20 characters. An alias cannot be **alias** or contain spaces.

command: Specifies a command string. Make sure the command string meets the syntax requirements.

Usage guidelines

System-defined command aliases cannot be deleted.

You can configure one or more aliases for a command or the starting keywords of commands. Then, you can use the aliases to execute the command or commands. If the command or commands have **undo** forms, you can also use the aliases to execute the **undo** command or commands.

For example, if you configure the alias **shiprt** for **display ip routing-table**, you can enter **shiprt** to execute the **display ip routing-table** command. If you configure the alias **ship** for **display ip**, you can use **ship** to execute all commands that start with **display ip**:

- Enter **ship routing-table** to execute the **display ip routing-table** command.
- Enter **ship interface** to execute the **display ip interface** command.

The command string can include up to nine parameters. Each parameter starts with the dollar sign ($) and a sequence number in the range of 1 to 9. For example, you can configure the alias **shinc** for the **display ip $1 | include $2** command. Then, to execute the **display ip routing-table | include Static** command, you only need to enter **shinc routing-table Static**. To execute the **display ip interface | include GigabitEthernet1/0/1** command, you only need to enter **shinc interface GigabitEthernet1/0/1**.

Examples

Configure **shiprt** as the alias for the **display ip routing-table** command and verify the configuration.

```
<Sysname> system-view
[Sysname] alias shiprt display ip routing-table
[Sysname] shiprt
Destinations : 13        Routes : 13
Destination/Mask   Proto   Pre Cost        NextHop         Interface
0.0.0.0/32         Direct  0   0           127.0.0.1       InLoop0
3.3.3.3/32         Static  60  0           192.168.1.62    Vlan1
127.0.0.0/8        Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32       Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32       Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
169.254.0.0/24     Direct  0   0           169.254.0.188   Vlan1
169.254.0.0/32     Direct  0   0           169.254.0.188   Vlan1
169.254.0.188/32   Direct  0   0           127.0.0.1       InLoop0
169.254.0.255/32   Direct  0   0           169.254.0.188   Vlan1
224.0.0.0/4        Direct  0   0           0.0.0.0         NULL0
224.0.0.0/24       Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
```

Configure **shinc** as the alias for **display ip $1 | include $2**.

```
[Sysname] alias shinc display ip $1 | include $2
```

Use alias **shinc** to display all static routes.

```
[Sysname] shinc routing-table Static
3.3.3.3/32         Static  60  0           192.168.1.62    Vlan1
```

Related commands

display alias

display [| [by-linenum] { begin | exclude | include }]

Use **display** [**|** [**by-linenum**] { **begin** | **exclude** | **include** }] to filter the output from a **display** command with regular expressions.

Syntax

display *command* [**|** [**by-linenum**] { **begin** | **exclude** | **include** } *regular-expression*]&<1-128>

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

command: Specifies the keywords and arguments of a **display** command. To display available keywords and arguments, enter **display ?**.

[**|** [**by-linenum**] { **begin** | **exclude** | **include** } *regular-expression*]&<1-128>: Specifies a maximum of 128 filter conditions.

- **by-linenum**: Numbers the output lines. You need to specify this keyword in only one filter condition.
- **begin**: Displays the first line matching the specified regular expression and all subsequent lines.
- **exclude**: Displays all lines not matching the specified regular expression.
- **include**: Displays all lines matching the specified regular expression.
- *regular-expression*: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Usage guidelines

To quickly locate certain lines in the output from a **display** command, you can use regular expressions to filter the output, and display a number before each output line. For more information about regular expressions, see *Fundamentals Configuration Guide*.

If you specify multiple filter conditions, the system displays the output lines that meet all the conditions.

A line number is a 5-character string and is typically followed by a colon (:). If you specify both the **by-linenum** and **begin** *regular-expression* options, a line number might be followed by a colon or a hyphen (-).

- **Colon**—The line matches the regular expression.
- **Hyphen**—The line does not match the regular expression.

Examples

Display the lines that contain **vlan** in the running configuration.

```
<Sysname> display current-configuration | include vlan
vlan 1
vlan 999
 port access vlan 999
```

Display log entries in the log buffer that contain both **SHELL** and **VTY**.

```
<Sysname> display logbuffer | include SHELL | include VTY
%Sep  6 10:38:12:320 2018 Sysname SHELL/5/SHELL_LOGIN: VTY logged in from 169.254.100.171.
%Sep  6 10:52:32:576 2018 Sysname SHELL/5/SHELL_LOGOUT: VTY logged out from
169.254.100.171.
%Sep  6 16:03:27:100 2018 Sysname SHELL/5/SHELL_LOGIN: VTY logged in from 169.254.100.171.
```

```
%Sep  6 16:44:18:113 2018 Sysname SHELL/5/SHELL_LOGOUT: VTY logged out from
169.254.100.171.
```

Display the running configuration, starting from the first line that contains **user-group** and numbering the output lines.

```
<Sysname> display current-configuration | by-linenum begin user-group
  114:  user-group system
  115-  #
  116-  return
```

display >

Use **display >** to save the output from a **display** command to a separate file.

Syntax

display *command* **>** *filename*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

command: Specifies the keywords and arguments of a **display** command. To display available keywords and arguments, enter **display ?**.

filename: Specifies the name of the file that is used to save the output, a string of 1 to 63 characters.

Usage guidelines

The **display** commands show the configuration, statistics, and states of the device. You can use the **display >** command to save the output to a file.

If the specified file does not exist, the system creates the file and saves the output to the file. If the file already exists, the system overwrites the file.

Examples

Save VLAN 1 settings to a separate file named **vlan.txt**.

```
<Sysname> display vlan 1 > vlan.txt
```

Check the content of the **vlan.txt** file.

```
<Sysname> more vlan.txt
VLAN ID: 1
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0001
 Name: VLAN 0001
 Tagged ports:   None
 Untagged ports:
    GigabitEthernet1/0/2
```

display >>

Use **display >>** to append the output from a **display** command to the end of a file.

Syntax

display *command* **>>** *filename*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

command: Specifies the keywords and arguments of a **display** command. To display available keywords and arguments, enter **display ?**.

filename: Specifies the name of the file that is used to save the output, a string of 1 to 63 characters.

Usage guidelines

The **display** commands show the configuration, statistics, and states of the device. You can use **display >>** to save the output to a file.

If the specified file does not exist, the system creates the file and saves the output to the file. If the file already exists, the system appends the output to the end of the file.

Examples

Append the VLAN 999 settings to the end of the **vlan.txt** file.

```
<Sysname> display vlan 999 >> vlan.txt
<Sysname>
```

Check the content of the **vlan.txt** file.

```
<Sysname> more vlan.txt
VLAN ID: 1
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0001
 Name: VLAN 0001
 Tagged ports:   None
 Untagged ports:
    GigabitEthernet1/0/2

 VLAN ID: 999
 VLAN type: Static
 Route interface: Configured
 IPv4 address: 192.168.2.1
 IPv4 subnet mask: 255.255.255.0
 Description: For LAN Access
 Name: VLAN 0999
 Tagged ports:   None
 Untagged ports:
```

```
GigabitEthernet1/0/2
```

display alias

Use **display alias** to display command aliases.

Syntax

display alias [*alias*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

alias: Specifies a command alias. If you do not specify this argument, the command displays all command aliases.

Examples

Display all command aliases.

```
<Sysname> display alias
Index     Alias               Command key
1         access-list         acl
2         end                 return
3         erase               delete
4         exit                quit
5         hostname            sysname
6         logging             info-center
7         no                  undo
8         shinc               display $1 | include $2
9         show                display
10        sirt                display ip routing-table
11        write               save
```

Display the command alias **shinc**.

```
<Sysname> display alias shinc
Alias               Command key
shinc               display ip $1 | include $2
```

Related commands

alias

display history-command

Use **display history-command** to display all commands that are saved in the command history buffer for the current CLI session.

Syntax

display history-command

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

The system automatically saves commands you have successfully executed to the command history buffer for the current CLI session. You can view them and execute them again.

By default, the system can save up to 10 commands in the buffer. You can use the **history-command max-size** command to change the buffer size. To buffer a new command when the buffer is full, the system deletes the oldest command entry in the buffer.

All commands in the command history buffer for the current CLI session will be cleared when you log out.

Examples

Display all commands saved in the command history buffer for the current CLI session.

```
<Sysname> display history-command
  system-view
  vlan 2
  quit
```

Related commands

history-command max-size

display history-command all

Use **display history-command all** to display all commands that are saved in the command history buffer for all CLI sessions.

Syntax

display history-command all

Views

Any view

Predefined user roles

network-admin

Usage guidelines

The system automatically saves commands successfully executed by users to the command history buffer for all CLI sessions. Users can view them but cannot recall them from the buffer.

Up to 1024 commands can be saved in the command history buffer. To buffer a new command when the buffer is full, the system deletes the oldest command entry in the buffer.

A user logout does not cause the system to delete commands from the history buffer for all CLI sessions.

Examples

Display all commands saved in the command history buffer for all CLI sessions.

```
<Sysname> display history-command all
  Date       Time     Terminal   Ip              User
```

```
03/16/2017 20:03:33 vty0       192.168.1.26    **
Cmd:dis his all

03/16/2017 20:03:29 vty0       192.168.1.26    **
Cmd:sys
```

Table 2 Command output

Field	Description
Date	Date when the command was executed.
Time	Time when the command was executed.
Terminal	User line used by the user.
Ip	IP address of the terminal used by the user.
User	Username used by the user if the user login authentication mode is **scheme**. If the login authentication mode is **none** or **password**, this field displays ******.
Cmd	Command string entered by the user.

Related commands

display history-command

display hotkey

Use **display hotkey** to display hotkey information.

Syntax

display hotkey

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display hotkey information.

```
<Sysname> display hotkey
----------------- Hotkeys -----------------
           -Defined function hotkeys-
CTRL_A  Move the cursor to the beginning of the line.
CTRL_B  Move the cursor one character to the left.
CTRL_C  Stop the current command.
CTRL_D  Erase the character at the cursor.
CTRL_E  Move the cursor to the end of the line.
CTRL_F  Move the cursor one character to the right.
CTRL_H  Erase the character to the left of the cursor.
CTRL_N  Display the next command in the history buffer.
CTRL_P  Display the previous command in the history buffer.
CTRL_R  Redisplay the current line.
```

```
CTRL_W  Delete the word to the left of the cursor.
CTRL_X  Delete all characters from the beginning of the line to the cursor.
CTRL_Y  Delete all characters from the cursor to the end of the line.
CTRL_Z  Return to the User View.
CTRL_]  Kill incoming connection or redirect connection.
ESC_B   Move the cursor back one word.
ESC_D   Delete all characters from the cursor to the end of the word.
ESC_F   Move the cursor forward one word.
           -Defined command hotkeys-
CTRL_G  display current-configuration
CTRL_L  display ip routing-table
CTRL_O  undo debugging all
           -Undefined hotkeys-
CTRL_T  NULL
CTRL_U  NULL
```

Related commands

hotkey

hotkey

Use **hotkey** to configure a hotkey.

Use **undo hotkey** to restore the default.

Syntax

hotkey *hotkey* { *command* | **function** *function* | **none** }

undo hotkey *hotkey*

Default

Table 3 shows the default definitions for hotkeys.

Table 3 Default definitions for hotkeys

Hotkey	Function or command
Ctrl+A	**move_the_cursor_to_the_beginning_of_the_line**: Moves the cursor to the beginning of a line.
Ctrl+B	**move_the_cursor_one_character_to_the_left**: Moves the cursor one character to the left.
Ctrl+C	**stop_the_current_command**: Stops the current command.
Ctrl+D	**erase_the_character_at_the_cursor**: Deletes the character at the cursor.
Ctrl+E	**move_the_cursor_to_the_end_of_the_line**: Moves the cursor to the end of a line.
Ctrl+F	**move_the_cursor_one_character_to_the_right**: Moves the cursor one character to the right.
Ctrl+G	**display current-configuration**: Displays the running configuration.
Ctrl+H	**erase_the_character_to_the_left_of_the_cursor**: Deletes the character to the left of the cursor.
Ctrl+L	**display ip routing-table**: Displays the IPv4 routing table information.

Ctrl+N	**display_the_next_command_in_the_history_buffer**: Displays the next command in the history buffer.
Ctrl+O	**`undo debugging all`**: Displays all debugging functions.
Ctrl+P	**display_the_previous_command_in_the_history_buffer**: Displays the previous command in the history buffer.
Ctrl+R	**redisplay_the_current_line**: Redisplays the current line.
Ctrl+T	N/A
Ctrl+U	N/A
Ctrl+W	**delete_the_word_to_the_left_of_the_cursor**: Deletes the word to the left of the cursor.
Ctrl+X	**delete_all_characters_from_the_beginning_of_the_line_to_the_cursor**: Deletes all characters to the left of the cursor.
Ctrl+Y	**delete_all_characters_from_the_cursor_to_the_end_of_the_line**: Deletes all characters from the cursor to the end of the line.
Ctrl+Z	**return_to_the_User_View**: Returns to user view.
Ctrl+]	**kill_incoming_connection_or_redirect_connection**: Terminates the current connection.
Esc+B	**move_the_cursor_back_one_word**: Moves the cursor back one word.
Esc+D	**delete_all_characters_from_the_cursor_to_the_end_of_the_word**: Deletes all characters from the cursor to the end of the word.
Esc+F	**move_the_cursor_forward_one_word**: Moves the cursor forward one word.

Views

System view

Predefined user roles

network-admin

Parameters

`hotkey`: Specifies a hotkey. To display the supported hotkeys, enter **`hotkey ?`** or see Table 3.

`command`: Specifies the command to be assigned to the hotkey.

`function` *`function`*: Specifies the function to be assigned to the hotkey. To display the supported functions, enter **`hotkey`** *`hotkey`* **`function ?`** or see Table 3.

none: Removes the command or function assignment for the hotkey. After you remove the assignment for a hotkey, pressing the hotkey does not execute any command or function.

Usage guidelines

The device supports a set of hotkeys. Pressing a hotkey executes the command or function assigned to the hotkey. You can configure all the hotkeys except **Ctrl+]**.

A hotkey can correspond to only one command or function. If you assign multiple commands or functions to the same hotkey, the most recently assigned command or function takes effect.

A command or function can be assigned to multiple hotkeys. You can use any of those hotkeys to execute the command or function.

If a hotkey is also defined by the terminal software you are using to interact with the device, the terminal software definition takes effect.

Examples

Assign the **display tcp statistics** command to hotkey **Ctrl+T**.

```
<Sysname> system-view
[Sysname] hotkey ctrl_t display tcp statistics
```

Assign move_the_cursor_to_the_beginning_of_the_line function to hotkey **Ctrl+U**.

```
<Sysname> system-view
[Sysname] hotkey ctrl_u function move_the_cursor_to_the_beginning_of_the_line
```

Disable the configurable command or function assigned to hotkey **Ctrl+A**.

```
<Sysname> system-view
[Sysname] hotkey ctrl_a none
```

Related commands

display hotkey

quit

Use **quit** to return to the upper-level view.

Syntax

quit

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

Executing this command in user view disconnects you from the device.

Examples

Return from GigabitEthernet 1/0/1 interface view to system view and then to user view.

```
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] quit
<Sysname>
```

repeat

Use **repeat** to repeat commands in the command history buffer for the current CLI session.

Syntax

repeat [*number*] [**count** *times*] [**delay** *seconds*]

Views

Any view

Predefined user roles

network-admin

Parameters

number: Specifies the number of the most recently executed commands in the command history buffer for the current CLI session that you want to execute. The value range is 1 to 10. The default is 1.

count *times*: Specifies the number of times that you want to execute the commands. The value range is 0 to 4294967295. The default is 0. If you do not specify this option, the system keeps executing the commands until you press the escape key to terminate the execution.

delay *seconds*: Specifies the time (in seconds) for the system to wait before executing the commands again. The value range is 0 to 4294967295. The default is 1.

Usage guidelines

To repeat a command, first enter the view for the command. To repeat multiple commands, first enter the view for the first command.

The **repeat** command executes commands in the order they were executed.

The system waits for your interaction when it repeats an interactive command.

Examples

Configure the system to execute the two most recently executed commands (**display cpu-usage** and **display clock**) three times at an interval of 10 seconds.

```
<Sysname> repeat 2 count 3 delay 10
<Sysname> display cpu
Slot 1 CPU 0 CPU usage:
      33% in last 5 seconds
      32% in last 1 minute
      33% in last 5 minutes
<Sysname> display clock
07:02:18.230 UTC Thu 06/19/2017
<Sysname> display cpu-usage
Slot 1 CPU 0 CPU usage:
      33% in last 5 seconds
      32% in last 1 minute
      33% in last 5 minutes
<Sysname> display clock
07:02:28.263 UTC Thu 06/19/2017
<Sysname> display cpu-usage
Slot 1 CPU 0 CPU usage:
      33% in last 5 seconds
      32% in last 1 minute
      33% in last 5 minutes
<Sysname> display clock
07:02:38.293 UTC Thu 06/19/2017
```

Related commands

display history-command

escape-key

history-command max-size

return

Use **return** to return to user view from any other view (except the Tcl configuration view and Python shell).

Syntax

return

Views

Any view except user view, Tcl configuration view, and Python shell

Predefined user roles

network-admin

network-operator

Usage guidelines

Pressing **Ctrl+Z** has the same effect as the **return** command, which can place you in to user view from any other view except the Tcl configuration view and Python shell.

To return to user view from Tcl configuration view, execute the **tclquit** command in Tcl configuration view.

To return to user view from the Python shell, execute the **exit()** command in the Python shell.

Examples

Return to user view from GigabitEthernet 1/0/1 interface view.

```
[Sysname-GigabitEthernet1/0/1] return
<Sysname>
```

screen-length disable

Use **screen-length disable** to disable pausing between screens of output for the current CLI session.

Use **undo screen-length disable** to enable pausing between screens of output for the current CLI session.

Syntax

screen-length disable

undo screen-length disable

Default

The default depends on the configuration of the **screen-length** command in user line view.

The following are the default settings for the **screen-length** command:

- Pausing between screens of output.
- Displaying up to 24 lines on a screen.

Views

User view

Predefined user roles

network-admin

Usage guidelines

If you disable pausing between screens of output, all output is displayed. The screen is refreshed continuously until the final screen is displayed.

This command takes effect only for the current CLI session. When you are logged out, the default is restored.

Examples

Disable pausing between screens of output for the current CLI session.

```
<Sysname> screen-length disable
```

Related commands

screen-length

system-view

Use **system-view** to enter system view from user view.

Syntax

system-view

Views

User view

Predefined user roles

network-admin

network-operator

Examples

Enter system view from user view.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname]
```

Contents

RBAC commands

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

description

Use **description** to configure a description for a user role for easy identification.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

A user role does not have a description.

Views

User role view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 128 characters.

Examples

Configure the description as **labVIP** for user role **role1**.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] description labVIP
```

Related commands

display role

role

display role

Use **display role** to display user role information.

Syntax

display role [**name** *role-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *role-name*: Specifies a user role name, a case-sensitive string of 1 to 63 characters. If you do not specify a user role name, the command displays information about all user roles, including the predefined user roles.

Examples

Display information about user role **123**.

```
<Sysname> display role name 123
Role: 123
  Description: new role
  VLAN policy: deny
  Permitted VLANs: 1 to 5, 7 to 8
  Interface policy: deny
  Permitted interfaces: GigabitEthernet1/0/1 to GigabitEthernet1/0/3, Vlan-interface1 to
Vlan-interface20
  VPN instance policy: permit (default)
  ------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ------------------------------------------------------------------
  1       permit RWX   feature-group abc
  2       deny   -W-   feature       ldap
  3       permit       command       system ; radius sc *
  4       permit R--   xml-element   -
  5       permit RW-   oid           1.2.1
  R:Read W:Write X:Execute
```

Display information about all user roles.

```
<Sysname> display role
Role: network-admin
  Description: Predefined network admin role has access to all commands on the
device
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ------------------------------------------------------------------
  sys-1   permit       command       *
  sys-2   permit RWX   web-menu      -
  sys-3   permit RWX   xml-element   -
  sys-4   deny         command       display security-logfile summary
  sys-5   deny         command       system-view ; info-center
                                     security-logfile directory *
  sys-6   deny         command       security-logfile save
  sys-7   permit RW-   oid           1
  R:Read W:Write X:Execute


Role: network-operator
  Description: Predefined network operator role has access to all read commands
on the device
```

```
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  sys-1   permit       command       display *
  sys-2   permit       command       xml
  sys-3   permit       command       system-view ; probe ; display *
  sys-4   deny         command       display history-command all
  sys-5   deny         command       display exception *
  sys-6   deny         command       display cpu-usage configuration
                                     *
  sys-7   deny         command       display kernel exception *
  sys-8   deny         command       display kernel deadloop *
  sys-9   deny         command       display kernel starvation *
  sys-10  deny         command       display kernel reboot *
  sys-13  permit       command       system-view ; local-user *
  sys-15  permit R--   web-menu      -
  sys-16  permit R--   xml-element   -
  sys-17  deny         command       display security-logfile summary
  sys-18  deny         command       system-view ; info-center
                                     security-logfile directory *
  sys-19  deny         command       security-logfile save
  sys-20  deny         command       system-view ; local-user-import
                                     *
  sys-21  deny         command       system-view ; local-user-export
                                     *
  sys-22  permit R--   oid           1
  R:Read W:Write X:Execute

Role: level-0
  Description: Predefined level-0 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  sys-1   permit       command       tracert *
  sys-2   permit       command       telnet *
  sys-3   permit       command       ping *
  sys-4   permit       command       ssh2 *
  sys-5   permit       command       super *
  sys-6   permit       command       mtrace *
  R:Read W:Write X:Execute

Role: level-1
```

```
  Description: Predefined level-1 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  sys-1   permit       command       tracert *
  sys-2   permit       command       telnet *
  sys-3   permit       command       ping *
  sys-4   permit       command       ssh2 *
  sys-5   permit       command       display *
  sys-6   permit       command       super *
  sys-7   deny         command       display history-command all
  sys-8   permit       command       mtrace *
  R:Read W:Write X:Execute

Role: level-2
  Description: Predefined level-2 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-3
  Description: Predefined level-3 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-4
  Description: Predefined level-4 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-5
  Description: Predefined level-5 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-6
  Description: Predefined level-6 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-7
```

```
  Description: Predefined level-7 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-8
  Description: Predefined level-8 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-9
  Description: Predefined level-9 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  sys-1   permit RWX   feature       -
  sys-2   deny   RWX   feature       device
  sys-3   deny   RWX   feature       filesystem
  sys-4   permit       command       display *
  sys-5   deny         command       display history-command all
  R:Read W:Write X:Execute

Role: level-10
  Description: Predefined level-10 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-11
  Description: Predefined level-11 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-12
  Description: Predefined level-12 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-13
  Description: Predefined level-13 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
```

```
  VPN instance policy: permit (default)

Role: level-14
  Description: Predefined level-14 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-15
  Description: Predefined level-15 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ------------------------------------------------------------------
  sys-1   permit       command       *
  sys-2   permit RWX   web-menu      -
  sys-3   permit RWX   xml-element   -
  sys-4   deny         command       display security-logfile summary
  sys-5   deny         command       system-view ; info-center
                                     security-logfile directory *
  sys-6   deny         command       security-logfile save
  sys-7   permit RW-   oid           1
  R:Read W:Write X:Execute

Role: security-audit
  Description: Predefined security audit role only has access to commands for
the security log administrator
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ------------------------------------------------------------------
  sys-1   deny         command       *
  sys-2   permit       command       display security-logfile summary
  sys-3   permit       command       system-view ; info-center
                                     security-logfile directory *
  sys-4   permit       command       security-logfile save
  sys-5   permit       command       cd *
  sys-6   permit       command       copy *
  sys-7   permit       command       delete *
  sys-8   permit       command       dir *
  sys-9   permit       command       mkdir *
  sys-10  permit       command       more *
  sys-11  permit       command       move *
  sys-12  permit       command       rmdir *
```

```
  sys-13  permit       command       pwd
  sys-14  permit       command       rename *
  sys-15  permit       command       undelete *
  sys-16  permit       command       ftp *
  sys-17  permit       command       sftp *
  R:Read W:Write X:Execute

Role: guest-manager
  Description: Predefined guest manager role can't access to commands
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ------------------------------------------------------------------
  sys-1   permit RWX   xml-element   useraccounts/approveguest/
  sys-2   permit RWX   xml-element   useraccounts/exportguestaccount/
  sys-3   permit RWX   xml-element   useraccounts/generateguestaccount/
  sys-4   permit RWX   xml-element   useraccounts/guest/
  sys-5   permit RWX   xml-element   useraccounts/guestconfigure/
  sys-6   permit RWX   xml-element   useraccounts/importguestaccount/
  sys-7   permit RWX   xml-element   useraccounts/exportguesttemplet/
  sys-8   permit RWX   xml-element   rpc/
  sys-9   deny         command       *
  R:Read W:Write X:Execute
```

Table 1 Command output

Field	Description
Role	User role name. Predefined user role names: • network-admin. • network-operator. • level-*n* (where *n* represents an integer in the range of 0 to 15). • security-audit. • guest-manager. This user role is not supported in the current software version.
Description	User role description.
VLAN policy	VLAN policy of the user role: • **deny**—Denies access to any VLANs except for permitted VLANs. • **permit (default)**—Default VLAN policy, which enables the user role to access all VLANs.
Permitted VLANs	VLANs accessible to the user role.
Interface policy	Interface policy of the user role: • **deny**—Denies access to any interfaces except for permitted interfaces. • **permit (default)**—Default interface policy, which enables the user role to access all interfaces.

Field	Description
Permitted interfaces	Interfaces accessible to the user role.
VPN instance policy	This field is not supported in the current software version. VPN instance policy of the user role: • **deny**—Denies access to any VPN instances except for permitted VPN instances. • **permit (default)**—Default VPN instance policy, which enables the user role to access all VPN instances.
Permitted VPN instances	This field is not supported in the current software version. VPN instances accessible to the user role.
Rule	User role rule number. Predefined user role rules are identified by sys-*n*, where *n* represents an integer.
Perm	Access control type: • **permit**—User role has access to the items in the **Entity** field. • **deny**—User role does not have access to the items in the **Entity** field.
Type	Controlled type: • **R**—Read-only. • **W**—Write. • **X**—Execute.
Scope	Rule control scope: • **command**—Controls access to the command or commands, as specified in the **Entity** field. • **feature**—Controls access to the commands of the feature, as specified in the **Entity** field. • **feature-group**—Controls access to the commands of the features in the feature group, as specified in the **Entity** field. • **web-menu**—Controls access to Web menus. • **xml-element**—Controls access to XML elements. • **oid**—Controls access to MIB nodes.
Entity	Command string, feature name, feature group, Web menu, XML element, or OID specified in the user role rule: • An en dash (–) represents any feature. • An asterisk (*) represents zero or more characters.

Related commands

`role`

display role feature

Use **`display role feature`** to display features available in the system.

Syntax

`display role feature` [**`name`** *`feature-name`* | **`verbose`**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *feature-name*: Specifies a feature by feature name. The *feature-name* argument represents the feature name, and all letters must be in lower case.

verbose: Displays the commands of each feature.

Usage guidelines

If you do not specify any parameters, the command displays only the list of features available in the system.

Examples

Display the list of feature names.

```
<Sysname> display role feature
Feature: device          (Device configuration related commands)
Feature: interface       (Interface related commands)
Feature: syslog          (Syslog related commands)
...
```

Display the commands of each feature.

```
<Sysname> display role feature verbose
Feature: device          (Device configuration related commands)
  display clock    (R)
  debugging dev    (W)
  display debugging dev    (R)
  display device *    (R)
  display diagnostic-information *    (R)
  display environment *    (R)
  display fan *    (R)
  display power *    (R)
  display current-configuration *    (R)
  display saved-configuration *    (R)
  display default-configuration *    (R)
  display startup    (R)
  display this *    (R)
...
```

Display the commands of feature **aaa**.

```
<Sysname> display role feature name aaa
Feature: aaa             (AAA related commands)
  system-view ; domain *    (W)
  system-view ; header *    (W)
  system-view ; aaa *    (W)
  display domain *    (R)
  display aaa *    (R)
  system-view ; user-group *    (W)
  system-view ; local-user *    (W)
  display local-user *    (R)
  display user-group *    (R)
```

```
  display debugging local-server    (R)
  debugging local-server *    (W)
  super *    (X)
  display password-control *    (R)
  reset password-control *    (W)
  system-view ; password-control *    (W)
...
```

Table 2 Command output (display role feature name aaa)

Field	Description
Feature	Displays the name and brief function description of the feature.
system-view ; domain *	All commands that start with the **domain** keyword in system view, and all commands in ISP domain view.
system-view ; header *	All commands that start with the **header** keyword in system view.
system-view ; aaa *	All commands that start with the **aaa** keyword in system view.
display domain *	All commands that start with the **display domain** keywords in user view.
system-view ; user-group *	All commands that start with the **user-group** keyword in system view, and all commands in user group view.
system-view ; local-user *	All commands that start with the **local-user** keyword in system view, and all commands in local user view.
display user-group *	All commands that start with the **display user-group** keywords in user view.
display debugging local-server	All commands that start with the **display debugging local-server** keywords in user view.
debugging local-server *	All commands that start with the **debugging local-server** keywords in user view.
super *	All commands that start with the **super** keyword in user view.
display password-control *	All commands that start with the **display password-control** keywords in user view.
reset password-control *	All commands that start with the **reset password-control** keywords in user view.
system-view ; password-control *	All commands that start with the **password-control** keyword in system view.
(W)	Command type is Write. A write command configures the system.
(R)	Command type is Read. A read command displays configuration or maintenance information.
(X)	Command type is Execute. An execute command executes a specific function.

Related commands

feature

display role feature-group

Use **display role feature-group** to display feature group information.

Syntax

display role feature-group [**name** *feature-group-name*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *feature-group-name*: Specifies a feature group. The *feature-group-name* argument represents the feature group name, a case-sensitive string of 1 to 31 characters. If you do not specify a feature group, the command displays information about all feature groups.

verbose: Displays the commands of each feature in feature groups. If you do not specify this keyword, the command displays only the feature lists of feature groups.

Usage guidelines

Feature groups **L2** and **L3** are predefined feature groups.

Examples

Display the feature lists of feature groups.

```
<Sysname> display role feature-group
Feature group: L2
Feature: igmp-snooping   (IGMP-Snooping related commands)
Feature: mld-snooping    (MLD-Snooping related commands)
Feature: lacp            (LACP related commands)
Feature: stp             (STP related commands)
Feature: lldp            (LLDP related commands)
Feature: dldp            (DLDP related commands)
Feature: cfm             (CFM related commands)
Feature: eoam            (EOAM related commands)
Feature: smart-link      (Smart-link related commands)
Feature: monitor-link    (Monitor-link related commands)
Feature: loopbk-detect   (Loopback-detection related commands)
Feature: vlan            (Virtual LAN related commands)
Feature: mvrp            (MVRP related commands )
Feature: rrpp            (RRPP related commands)
Feature: erps            (ERPS related commands)
Feature: ofp             (OFP related commands)
Feature: port-security   (Port-security related commands)
Feature: l2pt            (L2PT related commands)
Feature: dot1xc          (Dot1x client related commands)

Feature group: L3
Feature: route           (Route management related commands)
Feature: staticrt        (Unicast static route related commands)
```

```
Feature: ospf           (Open Shortest Path First protocol related commands)
Feature: rip            (Routing Information Protocol related commands)
Feature: lisp           (LISP protocol related commands)
Feature: route-policy   (Routing Policy related commands)
Feature: multicast      (Multicast related commands)
```

Display the commands in each feature group. For more information about the wildcards and marks used in the command list, see Table 2.

```
<Sysname> display role feature-group verbose
Feature group: L2
Feature: igmp-snooping   (IGMP-Snooping related commands)
  system-view ; igmp-snooping *    (W)
  system-view ; multicast-vlan *    (W)
  system-view ; user-profile * ; igmp-snooping *    (W)
  system-view ; vlan * ; igmp-snooping *    (W)
  system-view ; vlan * ; pim-snooping *    (W)
  system-view ; interface * ; igmp-snooping *    (W)
  system-view ; interface * ; port multicast-vlan *    (W)
  display igmp-snooping *    (R)
  display pim-snooping *    (R)
  display multicast-vlan *    (R)
  display l2-multicast *    (R)
  system-view ; probe ; display system internal l2-multicast *    (R)
  system-view ; probe ; display system internal multicast-vlan *    (R)
  reset igmp-snooping *    (W)
  reset pim-snooping *    (W)
  reset multicast-vlan *    (W)
  reset l2-multicast *    (W)
  debugging igmp-snooping *    (W)
  display debugging igmp-snooping *    (R)
  system-view ; probe ; debugging system internal igmp-snooping *    (W)
Feature: mld-snooping    (MLD-Snooping related commands)
  system-view ; mld-snooping *    (W)
  system-view ; ipv6 multicast-vlan *    (W)
  system-view ; user-profile * ; mld-snooping *    (W)
  system-view ; vlan * ; mld-snooping *    (W)
  system-view ; vlan * ; ipv6 pim-snooping *    (W)
  system-view ; interface * ; mld-snooping *    (W)
  system-view ; interface * ; ipv6 port multicast-vlan *    (W)
  display mld-snooping *    (R)
  display ipv6 pim-snooping *    (R)
  display ipv6 multicast-vlan *    (R)
  display ipv6 l2-multicast *    (R)
  system-view ; probe ; display system internal ipv6 l2-multicast *    (R)
  system-view ; probe ; display system internal ipv6 multicast-vlan *    (R)
  reset mld-snooping *    (W)
  reset ipv6 pim-snooping *    (W)
  reset ipv6 multicast-vlan *    (W)
  reset ipv6 l2-multicast *    (W)
```

```
  debugging mld-snooping *    (W)
  display debugging mld-snooping *    (R)
  system-view ; probe ; debugging system internal mld-snooping *    (W)
...
```

Display the feature list of the **L3** feature group.

```
<Sysname> display role feature-group name L3
Feature group: L3
Feature: route           (Route management related commands)
Feature: staticrt        (Unicast static route related commands)
Feature: ospf            (Open Shortest Path First protocol related commands)
Feature: rip             (Routing Information Protocol related commands)
Feature: lisp            (LISP protocol related commands)
Feature: route-policy    (Routing Policy related commands)
Feature: multicast       (Multicast related commands)
```

Related commands

`feature`

`role feature-group`

feature

Use **`feature`** to add a feature to a feature group.

Use **`undo feature`** to remove a feature from a feature group.

Syntax

`feature` *`feature-name`*

`undo feature` *`feature-name`*

Default

A user-defined feature group does not have any features.

Views

Feature group view

Predefined user roles

network-admin

Parameters

`feature-name`: Specifies a feature name. You must enter the feature name in lower case.

Usage guidelines

Repeat the **`feature`** command to add multiple features to a feature group.

Examples

Add the AAA and ACL features to feature group **security-features**.

```
<Sysname> system-view
[Sysname] role feature-group name security-features
[Sysname-featuregrp-security-features] feature aaa
[Sysname-featuregrp-security-features] feature acl
```

Related commands

display role feature

display role feature-group

role feature-group

interface policy deny

Use **interface policy deny** to enter user role interface policy view.

Use **undo interface policy deny** to restore the default.

Syntax

interface policy deny

undo interface policy deny

Default

A user role has access to all interfaces.

Views

User role view

Predefined user roles

network-admin

Usage guidelines

CAUTION:

This command denies the access of the user role to any interfaces if you do not specify accessible interfaces by using the **permit interface** command. To configure an interface, make sure the interface is permitted by the user role interface policy in use.

To restrict the interface access of a user role to a set of interfaces, perform the following tasks:

1. Use **interface policy deny** to enter user role interface policy view.
2. Use **permit interface** to specify accessible interfaces.

You can perform the following tasks on an accessible interface:

- Create, remove, or configure the interface.
- Enter interface view.
- Specify the interface in feature commands.

The create and remove operations are available only for logical interfaces.

Any change to a user role interface policy takes effect only on users who log in with the user role after the change.

Examples

Enter user role interface policy view of **role1**, and deny **role1** to access any interfaces.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] interface policy deny
[Sysname-role-role1-ifpolicy] quit
```

Enter user role interface policy view of **role1**, and deny **role1** to access any interfaces except for GigabitEthernet 1/0/1 to GigabitEthernet 1/0/4.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] interface policy deny
[Sysname-role-role1-ifpolicy] permit interface gigabitethernet 1/0/1 to gigabitethernet
1/0/4
```

Related commands

display role

permit interface

role

permit interface

Use **permit interface** to configure a list of interfaces accessible to a user role.

Use **undo permit interface** to disable the access of a user role to specific interfaces.

Syntax

permit interface *interface-list*

undo permit interface [*interface-list*]

Default

No permitted interfaces are configured in user role interface policy view.

Views

User role interface policy view

Predefined user roles

network-admin

Parameters

interface-list: Specifies a space-separated list of up to 10 interface items. Each interface item specifies one interface in the *interface-type interface-number* form or a range of interfaces in the *interface-type interface-number* **to** *interface-type interface-number* form. If you specify an interface range, the end interface must meet the following requirements:

- Be the same type as the start interface.
- Have a higher interface number than the start interface.

Usage guidelines

To permit a user role to access an interface after you configure the **interface policy deny** command, you must add the interface to the permitted interface list of the policy. With the user role, you can perform the following tasks to the interfaces in the permitted interface list:

- Create, remove, or configure the interfaces.
- Enter the interface views.
- Specify the interfaces in feature commands.

The create and remove operations are available only for logical interfaces.

You can repeat the **permit interface** command to add multiple permitted interfaces to a user role interface policy.

The **undo permit interface** command removes the entire list of permitted interfaces if you do not specify an interface.

Any change to a user role interface policy takes effect only on users who log in with the user role after the change.

Examples

1. Configure user role **role1**:

Permit user role **role1** to execute all commands available in interface view and VLAN view.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] rule 1 permit command system-view ; interface *
[Sysname-role-role1] rule 2 permit command system-view ; vlan *
```

Permit the user role to access GigabitEthernet 1/0/1, and GigabitEthernet 1/0/3 to GigabitEthernet 1/0/5.

```
[Sysname-role-role1] interface policy deny
[Sysname-role-role1-ifpolicy] permit interface gigabitethernet 1/0/1
gigabitethernet 1/0/3 to gigabitethernet 1/0/5
[Sysname-role-role1-ifpolicy] quit
[Sysname-role-role1] quit
```

2. Verify that you cannot use user role **role1** to work on any interfaces except for GigabitEthernet 1/0/1 and GigabitEthernet 1/0/3 to GigabitEthernet 1/0/5:

Verify that you can enter GigabitEthernet 1/0/1 interface view.

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] quit
```

Verify that you can assign GigabitEthernet 1/0/5 to VLAN 10. In this example, the user role can access all VLANs because the default VLAN policy of the user role is used.

```
[Sysname] vlan 10
[Sysname-vlan10] port gigabitethernet 1/0/5
[Sysname-vlan10] quit
```

Verify that you cannot enter interface view of GigabitEthernet 1/0/2.

```
[Sysname] interface gigabitethernet 1/0/2
Permission denied.
```

Related commands

display role

interface policy deny

role

permit vlan

Use **permit vlan** to configure a list of VLANs accessible to a user role.

Use **undo permit vlan** to remove the permission for a user role to access specific VLANs.

Syntax

permit vlan *vlan-id-list*

undo permit vlan [*vlan-id-list*]

Default

No permitted VLANs are configured in user role VLAN policy view.

Views

User role VLAN policy view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 VLAN items. Each VLAN item specifies a VLAN by VLAN ID or specifies a range of VLANs in the form of *vlan-id1* **to** *vlan-id2*. The value range for the VLAN IDs is 1 to 4094. If you specify a VLAN range, the value for the *vlan-id2* argument must be greater than the value for the *vlan-id1* argument.

Usage guidelines

To permit a user role to access a VLAN after you configure the **vlan policy deny** command, you must add the VLAN to the permitted VLAN list of the policy. With the user role, you can perform the following tasks on the VLANs in the permitted VLAN list:

- Create, remove, or configure the VLANs.
- Enter the VLAN views.
- Specify the VLANs in feature commands.

You can repeat the **permit vlan** command to add multiple permitted VLANs to a user role VLAN policy.

The **undo permit vlan** command removes the entire list of permitted VLANs if you do not specify a VLAN.

Any change to a user role VLAN policy takes effect only on users who log in with the user role after the change.

By default, all access ports belong to VLAN 1. To assign an access port to any other VLAN by using the **port access vlan** command, make sure you have a user role that can access both VLAN 1 and the new VLAN.

Examples

1. Configure user role **role1**:

Permit user role **role1** to execute all commands available in interface view and VLAN view.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] rule 1 permit command system-view ; interface *
[Sysname-role-role1] rule 2 permit command system-view ; vlan *
```

Permit user role **role1** to access VLANs 1, 2, 4, and 50 to 100.

```
[Sysname-role-role1] vlan policy deny
[Sysname-role-role1-vlanpolicy] permit vlan 1 2 4 50 to 100
[Sysname-role-role1-vlanpolicy] quit
[Sysname-role-role1] quit
```

2. Verify that you cannot use user role **role1** to work on any VLANs except for VLANs 1, 2, 4, and 50 to 100:

Verify that you can create VLAN 100 and enter VLAN view.

```
[Sysname] vlan 100
[Sysname-vlan100] quit
```

Verify that you can add GigabitEthernet 1/0/1 to VLAN 100 as an access port.

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port access vlan 100
[Sysname-GigabitEthernet1/0/1] quit
```

Verify that you cannot create VLAN 101 or enter VLAN view.

```
[Sysname] vlan 101
```

```
Permission denied.
```

Related commands

display role

role

vlan policy deny

role

Use **role** to create a user role and enter its view, or enter the view of an existing user role.

Use **undo role** to delete a user role.

Syntax

role name *role-name*

undo role name *role-name*

Default

The system has the following predefined user roles: network-admin, network-operator, level-*n* (where *n* represents an integer in the range of 0 to 15), and security-audit.

Views

System view

Predefined user roles

network-admin

Parameters

name *role-name*: Specifies a username. The *role-name* argument is a case-sensitive string of 1 to 63 characters.

Usage guidelines

You can create a maximum of 64 user roles in addition to the predefined user roles.

You cannot delete the predefined user roles or change the permissions assigned to network-admin, network-operator, level-15, or security-audit.

You cannot assign the security-audit user role to non-AAA authentication users.

The access permissions of the level-0 to level-14 user roles can be modified through user role rules and resource access policies. However, you cannot make changes on the predefined access permissions of these user roles. For example, you cannot change the access permission of these user roles to the **display history-command all** command.

Examples

Create user role **role1** and enter its view.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1]
```

Related commands

display role

interface policy deny

rule

vlan policy deny

role default-role enable

Use **role default-role enable** to enable the default user role feature for remote AAA users.

Use **undo role default-role enable** to restore the default.

Syntax

role default-role enable [*role-name*]

undo role default-role enable

Default

The default user role feature is disabled. AAA users who do not have a user role cannot log in to the device.

Views

System view

Predefined user roles

network-admin

Parameters

role-name: Specifies a user role by its name for the default user role. The user role must already exist. The argument is a case-sensitive string of 1 to 63 characters.

Usage guidelines

The default user role feature assigns the default user role to AAA-authenticated users if the authentication server (local or remote) does not assign any user roles to the users. These users are allowed to access the system with the default user role.

For local authorization, this command is required if you do not use the **authorization-attribute user role** command to assign user roles to local users.

If AAA users have been assigned user roles, they log in with the user roles.

If you do not specify the *role-name* argument, the default user role is network-operator.

Examples

Enable the default user role feature.

```
<Sysname> system-view
[Sysname] role default-role enable
```

Related commands

role

role feature-group

Use **role feature-group** to create a user role feature group and enter its view, or enter the view of an existing user role feature group.

Use **undo role feature-group** to delete a user role feature group.

Syntax

role feature-group name *feature-group-name*

undo role feature-group name *feature-group-name*

Default

Two user role feature groups **L2** and **L3** exist.

Views

System view

Predefined user roles

network-admin

Parameters

name *feature-group-name*: Specifies a feature group name. The *feature-group-name* argument is a case-sensitive string of 1 to 31 characters.

Usage guidelines

The **L2** feature group includes all Layer 2 feature commands, and the **L3** feature group includes all Layer 3 feature commands. These predefined feature groups are not user configurable.

In addition to the predefined feature groups **L2** and **L3**, you can create a maximum of 64 user role feature groups.

Examples

Create feature group **security-features** and enter its view.

```
<Sysname> system-view
[Sysname] role feature-group name security-features
[Sysname-featuregrp-security-features]
```

Related commands

display role feature

display role feature-group

feature

rule

Use **rule** to create or change a user role rule.

Use **undo rule** to delete user role rules.

Syntax

rule *number* { **deny** | **permit** } { **command** *command-string* | { **execute** | **read** | **write** } * { **feature** [*feature-name*] | **feature-group** *feature-group-name* | **oid** *oid-string* | **web-menu** [*web-string*] | **xml-element** [*xml-string*] } }

undo rule { *number* | **all** }

Default

A user-defined user role does not have any rules and cannot access any resources.

Views

User role view

Predefined user roles

network-admin

Parameters

number: Specifies a rule number in the range of 1 to 256.

deny: Denies access to the specified commands, Web menus, XML elements, or MIB nodes.

permit: Permits access to the specified commands, Web menus, XML elements, or MIB nodes.

command *command-string*: Specifies a command string. The command string can represent a command or a group of commands. The *command-string* argument is a case-sensitive string of 1 to 128 characters, including the following characters:

- The wildcard asterisk (*).
- The delimiters space and tab.
- All printable characters.

execute: Specifies the execute commands, Web menus, XML elements, or MIB nodes to execute a specific function or program. The **ping** command is an example of execute commands.

read: Specifies the read commands, Web menus, XML elements, or MIB nodes to display configuration or maintenance information. The **display**, **dir**, **more**, and **pwd** commands are examples of read commands.

write: Specifies the write commands, Web menus, XML elements, or MIB nodes to configure the system. The **ssh server enable** command is an example of write commands.

feature [*feature-name*]: Specifies one or all features. The *feature-name* argument is a case-sensitive character string. If you do not specify a feature name, you specify all the features in the system.

feature-group *feature-group-name*: Specifies a user-defined or predefined feature group. The *feature-group-name* argument represents the feature group name, a case-sensitive string of 1 to 31 characters. If the feature group has not been created, the rule takes effect after the group is created. To display the feature groups that have been created, use the **display role feature-group** command.

oid *oid-string*: Specifies an OID of a MIB node. The *oid-string* argument represents the OID, a case-insensitive string of 1 to 255 characters. The OID is a dotted numeric string that uniquely identifies the path from the root node to this node. For example, 1.3.6.1.4.1.25506.8.35.14.19.1.1.

web-menu [*web-string*]: Specifies a Web menu. The *web-string* argument represents the ID path of the Web menu, a case-insensitive string of 1 to 255 characters. Use the forward slash (/) to separate ID items, for example, M_DEVICE/I_BASIC_INFO/I_reboot. If you do not specify a Web menu, the rule applies to all Web items. To verify the ID path of a Web menu, use the **display web menu** command.

xml-element [*xml-string*]: Specifies an XML element. The *xml-string* argument represents the XPath of the XML element, a case-insensitive string of 1 to 255 characters. Use the forward slash (/) to separate Xpath items, for example, Interfaces/Index/Name. If you do not specify an XML element, the rule applies to all XML elements.

all: Specifies all the user role rules.

Usage guidelines

You can define the following types of rules for different access control granularities:

- **Command rule**—Controls access to a command or a set of commands that match a regular expression.
- **Feature rule**—Controls access to the commands of a feature by command type.
- **Feature group rule**—Controls access to the commands of a group of features by command type.
- **Web menu rule**—Controls access to Web menus by menu type.
- **XML element rule**—Controls access to XML elements by element type.
- **OID rule**—Controls access to the specified MIB node and its child nodes by node type.

A user role can access the set of permitted resources specified in the user role rules. User role rules include predefined (identified by sys-n) and user-defined user role rules.

You can configure a maximum of 256 user-defined rules for a user role. The total number of user-defined user role rules cannot exceed 1024.

Any rule modification, addition, or removal for a user role takes effect only on the users who log in with the user role after the change.

Access to the file system commands is controlled by both the file system command rules and the file system feature rule.

A command with output redirection to the file system is permitted only when the command type write is assigned to the file system feature.

The following guidelines apply to non-OID rules:

- If two user-defined rules of the same type conflict, the rule with the higher ID takes effect. For example, a user role can use the **`tracert`** command but not the **`ping`** command if the user role contains rules configured by using the following commands:
  - **`rule`** *`1`* **`permit command`** *`ping`*
  - **`rule`** *`2`* **`permit command`** *`tracert`*
  - **`rule`** *`3`* **`deny command`** *`ping`*
- If a predefined user role rule and a user-defined user role rule conflict, the user-defined user role rule takes effect.

The following guidelines apply to OID rules:

- The system compares an OID with the OIDs specified in rules, and it uses the longest match principle to select a rule for the OID. For example, a user role cannot access the MIB node with OID 1.3.6.1.4.1.25506.141.3.0.1 if the user role contains rules configured by using the following commands:
  - **`rule`** *`1`* **`permit read write oid`** *`1.3.6`*
  - **`rule`** *`2`* **`deny read write oid`** *`1.3.6.1.4.1`*
  - **`rule`** *`3`* **`permit read write oid`** *`1.3.6.1.4`*
- If the same OID is specified in multiple rules, the rule with the higher ID takes effect. For example, a user role can access the MIB node with OID 1.3.6.1.4.1.25506.141.3.0.1 if the user role contains rules configured by using the following commands:
  - **`rule`** *`1`* **`permit read write oid`** *`1.3.6`*
  - **`rule`** *`2`* **`deny read write oid`** *`1.3.6.1.4.1`*
  - **`rule`** *`3`* **`permit read write oid`** *`1.3.6.1.4.1`*

When you specify a command string, follow the guidelines in Table 3.

Table 3 Command string configuration rules

Rule	Guidelines
Semicolon (;) is the delimiter.	Use a semicolon to separate the command of each view that you must enter before you access a command or a set of commands. However, do not use a semicolon to separate commands available in user view or any view, for example, **display** and **dir**. Each semicolon-separated segment must have a minimum of one printable character. To specify the commands in a view but not the commands in the view's subviews, use a semicolon as the last printable character in the last segment. To specify the commands in a view and the view's subviews, the last printable character in the last segment must not be a semicolon. For example, you must enter system view before you enter interface view. To specify all commands starting with the **ip** keyword in any interface view, you must use the "system ; interface * ; ip * ;" command string. For another example, the "system ; radius scheme * ;" command string represents all commands that start with the **radius scheme** keywords in system view. The "system ; radius scheme *" command string represents all commands that start with the **radius scheme** keywords in system view and all commands in RADIUS scheme view.
Asterisk (*) is the wildcard.	An asterisk represents zero or multiple characters. In a non-last segment, you can use an asterisk only at the end of the segment. In the last segment, you can use an asterisk in any position of the segment. If the asterisk appears at the beginning, you cannot specify a printable character behind the asterisk. For example, the "system ; *" command string represents all commands available in system view and all subviews of the system view. The "debugging * event" command string represents all event debugging commands available in user view.
Keyword abbreviation is allowed.	You can specify a keyword by entering the first few characters of the keyword. Any command that starts with this character string matches the rule. For example, "rule 1 deny command dis arp source *" denies access to the commands **display arp source-mac interface** and **display arp source-suppression**.
To control the access to a command, you must specify the command immediately after the view that has the command.	To control access to a command, you must specify the command immediately behind the view to which the command is assigned. The rules that control command access for any subview do not apply to the command. For example, the "rule 1 deny command system ; interface * ; *" command string disables access to any command that is assigned to interface view. However, you can still execute the **acl advanced** command in interface view, because this command is assigned to system view rather than interface view. To disable access to this command, use "rule 1 deny command system ; acl *;".
Do not include the vertical bar (|), greater-than sign (>), or double greater-than sign (>>) when you specify **display** commands in a user role command rule.	The system does not treat the redirect signs and the parameters that follow the signs as part of command lines. However, in user role command rules, these redirect signs and parameters are handled as part of command lines. As a result, no rule that includes any of these signs can find a match. For example, "rule 1 permit command display debugging > log" can never find a match. This is because the system has a **display debugging** command but not a **display debugging > log** command.

Examples

Permit user role **role1** to execute the **display acl** command.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] rule 1 permit command display acl
```

Permit user role **role1** to execute all commands that start with the **display** keyword.

```
[Sysname-role-role1] rule 2 permit command display *
```

Permit user role **role1** to execute the **radius scheme aaa** command in system view and use all commands assigned to RADIUS scheme view.

```
[Sysname-role-role1] rule 3 permit command system ; radius scheme aaa
```

Deny the access of **role1** to the read or write commands of any features.

```
[Sysname-role-role1] rule 4 deny read write feature
```

Deny the access of **role1** to the read commands of the **aaa** feature.

```
[Sysname-role-role1] rule 5 deny read feature aaa
```

Permit **role1** to access all read, write, and execute commands of feature group **security-features**.

```
[Sysname-role-role1] rule 6 permit read write execute feature-group security-features
```

Permit **role1** to access all read and write MIB nodes starting from the node with OID 1.1.2.

```
[Sysname-role-role1] rule 7 permit read write oid 1.1.2
```

Related commands

display role

display role feature

display role feature-group

display web menu

role

super

Use **super** to obtain another user role without reconnecting to the device.

Syntax

super [*role-name*]

Views

User view

Predefined user roles

network-admin

Parameters

role-name: Specifies a user role, a case-sensitive string of 1 to 63 characters. The user role must exist in the system and cannot be security-audit. If you do not specify a user role, you obtain the default target user role which is set by using the **super default role** command.

Usage guidelines

The obtained user role is a temporary user role, because this command is effective only on the current login. The next time you are logged in with the user account, the original user role settings take effect.

To enable a user to obtain another user role without reconnecting to the device, you must configure user role authentication.

- If no local password is configured in the local password authentication (**local**), an AUX user can obtain the user role by either entering a string or not entering anything.
- If no local password is configured in the local-then-remote authentication (**local scheme**), the following rules apply:
  - A VTY user performs remote authentication.
  - An AUX user can obtain user role authorization by either entering a string or not entering anything.

Examples

Obtain the user role network-operator.

```
<Sysname> super network-operator
Password:
User privilege role is network-operator, and only those commands that authorized to the role can be used.
```

Related commands

authentication super (*Security Command Reference*)

super authentication-mode

super password

super authentication-mode

Use **super authentication-mode** to set an authentication mode for temporary user role authorization.

Use **undo super authentication-mode** to restore the default.

Syntax

super authentication-mode { **local** | **scheme** } *

undo super authentication-mode

Default

Local password authentication applies.

Views

System view

Predefined user roles

network-admin

Parameters

local: Enables local password authentication.

scheme: Enables remote AAA authentication.

Usage guidelines

For local password authentication, use the **super password** command to set a password.

For remote AAA authentication, set the username and password on the RADIUS or HWTACACS server.

If you specify both **local** and **scheme** keywords, the keyword first entered in the command takes precedence.

- **scheme local**—Enables remote-then-local authentication mode. The device first performs AAA authentication to obtain a temporary user role. Local password authentication is performed if the remote HWTACACS or RADIUS server does not respond, or if the AAA configuration on the device is invalid.
- **local scheme**—Enables local-then-remote authentication mode. The device first performs local password authentication. If no password is configured for the user role, the device performs remote authentication for VTY users. An AUX user can obtain another user role by either entering a string or not entering anything.

For more information about AAA, see *Security Configuration Guide*.

Examples

Enable local-only authentication for temporary user role authorization.

```
<Sysname> system-view
[Sysname] super authentication-mode local
```

Enable remote-then-local authentication for temporary user role authorization.

```
<Sysname> system-view
[Sysname] super authentication-mode scheme local
```

Related commands

authentication super (*Security Command Reference*)

super password

super default role

Use **super default role** to specify the default target user role for temporary user role authorization.

Use **undo super default role** to restore the default.

Syntax

super default role *role-name*

undo super default role

Default

The default target user role is network-admin.

Views

System view

Predefined user roles

network-admin

Parameters

role-name: Specifies the name of the default target user role, a case-sensitive string of 1 to 63 characters. The user role must exist in the system and cannot be security-audit.

Usage guidelines

The default target user role is applied to the **super** or **super password** command when you do not specify a user role for the command.

Examples

Specify **network-operator** as the default target user role for temporary user role authorization.

```
<Sysname> system-view
```

```
[Sysname] super default role network-operator
```

Related commands

super

super password

super password

Use **super password** to set a password for a user role.

Use **undo super password** to delete the password for a user role.

Syntax

In non-FIPS mode:

super password [**role** *role-name*] [{ **hash** | **simple** } *string*]

undo super password [**role** *role-name*]

In FIPS mode:

super password [**role** *role-name*]

undo super password [**role** *role-name*]

Default

No password is set for a user role.

Views

System view

Predefined user roles

network-admin

Parameters

role *role-name*: Specifies a user role, a case-sensitive string of 1 to 63 characters. The user role must exist in the system and cannot be security-audit. If you do not specify a user role, the command sets a password for the default target user role which is set by using the **super default role** command.

hash: Specifies a password in hashed form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in hashed form.

string: Specifies the password. In non-FIPS mode, the plaintext form of the password is a case-sensitive string of 1 to 63 characters. The hashed form of the password is a case-sensitive string of 1 to 110 characters. In FIPS mode, the password must be a case-sensitive plaintext string of 15 to 63 characters. The string must contain four character types including digits, uppercase letters, lowercase letters, and special characters.

Usage guidelines

If you do not specify any parameters, you specify a plaintext password in the interactive mode.

The FIPS mode supports only the interactive mode for setting a password.

Set a password if you configure local password authentication for temporary user role authorization.

It is a good practice to specify different passwords for different user roles.

When the global password control feature is enabled, all history super passwords are stored in hashed form.

- If you set a new super password in plaintext form, make sure the new super password is different from the current one and those stored in the history super password records.
- If you set a new super password in hashed form, the system does not compare the new super password with the current one or those stored in the history super password records.

Examples

Set the password to **123456TESTplat&!** in plaintext form for user role network-operator.

```
<Sysname> system-view
[Sysname] super password role network-operator simple 123456TESTplat&!
```

Set the password to **123456TESTplat&!** in the interactive mode for user role network-operator.

```
<Sysname> system-view
[Sysname] super password role network-operator
Password:
Confirm :
Updating user information. Please wait... ...
```

Related commands

super authentication-mode

super default role

super use-login-username

Use **super use-login-username** to enable the device to automatically obtain the login username when a login user requests temporary user role authorization from a remote authentication server.

Use **undo super use-login-username** to restore the default.

Syntax

super use-login-username

undo super use-login-username

Default

The device prompts for a username when a login user requests temporary user role authorization from a remote authentication server.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command is applicable only to the login from a user line that uses scheme authentication, which requires a username for login.

If the user was logged in from a user line that uses password authentication or no authentication, the device cannot obtain the login username. The request for temporary user role authorization from a remote authentication server will fail.

This command does not take effect on local password authentication for temporary user role authorization.

Examples

Enable the device to automatically obtain the login username when a login user requests temporary user role authorization from a remote authentication server.

```
<Sysname> system-view
[Sysname] super use-login-username
```

Related commands

authentication super (*Security Command Reference*)

super authentication-mode

super password

vlan policy deny

Use **vlan policy deny** to enter user role VLAN policy view.

Use **undo vlan policy deny** to restore the default.

Syntax

vlan policy deny

undo vlan policy deny

Default

A user role has access to all VLANs.

Views

User role view

Predefined user roles

network-admin

Usage guidelines

CAUTION:

The **vlan policy deny** command denies the access of the user role to any VLANs if you do not specify accessible VLANs by using the **permit vlan** command. To configure a VLAN, make sure the VLAN is permitted by the user role VLAN policy in use.

To restrict the VLAN access of a user role to a set of VLANs, perform the following tasks:

1. Use **vlan policy deny** to enter user role VLAN policy view.
2. Use **permit vlan** to specify accessible VLANs.

You can perform the following tasks on an accessible VLAN:

- Create, remove, or configure the VLAN.
- Enter VLAN view.
- Specify the VLAN in feature commands.

Any change to a user role VLAN policy takes effect only on users who log in with the user role after the change.

Examples

Enter user role VLAN policy view of **role1**, and deny the access of **role1** to any VLANs.

```
<Sysname> system-view
[Sysname] role name role1
```

```
[Sysname-role-role1] vlan policy deny
[Sysname-role-role1-vlanpolicy] quit
```

Enter user role VLAN policy view of **role1**, and deny the access of **role1** to any VLANs except for VLANs 50 to 100.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] vlan policy deny
[Sysname-role-role1-vlanpolicy] permit vlan 50 to 100
```

Related commands

display role

permit vlan

role

Contents

Login management commands

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

Some login management commands are available in both user line view and user line class view. For these commands, the device uses the following rules to determine the settings to be activated:

- A setting in user line view applies only to the user line. A setting in user line class view applies to all user lines of the class.
- A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.
- A setting in user line class view takes effect for login sessions that are established after the setting is configured.

activation-key

Use **activation-key** to set the terminal session activation key. Pressing this shortcut key starts a terminal session.

Use **undo activation-key** to restore the default.

Syntax

activation-key *key-string*

undo activation-key

Default

The terminal session activation key is **Enter**.

Views

User line view

User line class view

Predefined user roles

network-admin

Parameters

key-string: Specifies a shortcut key. It can be a character (case sensitive), or an ASCII code value in the range of 0 to 127. For example, if you configure **activation-key 1**, the shortcut key is **Ctrl+A**. If you configure **activation-key a**, the shortcut key is **a**. For information about ASCII code values of individual characters, see the standard ASCII code chart. For information about ASCII code values of combined keys that use the **Ctrl** key, see Table 1.

Usage guidelines

This command is not supported in VTY line view or VTY line class view.

This command takes effect immediately.

This command is available in both user line view and user line class view. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.

You can use only the specified terminal session activation key to start a terminal session. To display the current terminal session activation key, use the **`display current-configuration | include activation-key`** command.

Table 1 ASCII code values for combined keys that use the Ctrl key

Combined key	ASCII code value
Ctrl+A	1
Ctrl+B	2
Ctrl+C	3
Ctrl+D	4
Ctrl+E	5
Ctrl+F	6
Ctrl+G	7
Ctrl+H	8
Ctrl+I	9
Ctrl+J	10
Ctrl+K	11
Ctrl+L	12
Ctrl+M	13
Ctrl+N	14
Ctrl+O	15
Ctrl+P	16
Ctrl+Q	17
Ctrl+R	18
Ctrl+S	19
Ctrl+T	20
Ctrl+U	21
Ctrl+V	22
Ctrl+W	23
Ctrl+X	24
Ctrl+Y	25
Ctrl+Z	26
CTRL+ [	27
CTRL+\	28
CTRL+]	29
CTRL+^	30
CTRL+_	31

Examples

Configure character **s** as the terminal session activation key for AUX line 0.

```
<Sysname> system-view
[Sysname] line aux 0
[Sysname-line-aux0] activation-key s
```

To verify the configuration:

1. Exit the AUX session.

   ```
   [Sysname-line-aux0] return
   <Sysname> quit
   ```

2. Log in again through the AUX line.

   The following message appears:

   ```
   Press ENTER to get started.
   ```

3. Press **Enter**.

   Pressing **Enter** does not start a session.

4. Press **s**.

   A terminal session is started.

   ```
   <Sysname>
   ```

authentication-mode

Use **authentication-mode** to set the authentication mode for a user line.

Use **undo authentication-mode** to restore the default.

Syntax

In non-FIPS mode:

authentication-mode { **none** | **password** | **scheme** }

undo authentication-mode

In FIPS mode:

authentication-mode scheme

undo authentication-mode

Default

In non-FIPS mode:

- The authentication mode is **password** for a VTY line.
- The authentication mode for console login depends on the device model.
  - On the S5000V3-EI, S5000V5-EI, S5000E-X, S5000X-EI, and WAS6000 switch series, the default setting varies by startup configuration.
    - If the device starts up with factory defaults, the authentication mode is **scheme**.
    - If the device starts up with the initial configuration, the authentication mode is **none**.
  - On the other switch series, the authentication mode is **none**.

In FIPS mode:

The authentication mode is **scheme**.

Views

User line view

User line class view

Predefined user roles

network-admin

Parameters

none: Disables authentication.

password: Performs local password authentication.

scheme: Performs AAA authentication. For more information about AAA, see *Security Configuration Guide*.

Usage guidelines

CAUTION:

- When authentication is disabled, users can login without authentication. For security purpose, disable authentication with caution.
- When you enable password authentication, you must also configure an authentication password for the line or line class. If no authentication password is configured, you cannot log in to the device through the line or line class at the next time.
- When you enable scheme authentication, make sure an authentication user account is available. If no authentication user account is available, you cannot log in to the device through the line or line class at the next time.

Only users assigned the network-admin, or level-15 user role can execute this command. Other users cannot execute this command, even if they are granted the right to execute this command.

In VTY line view, this command is associated with the **protocol inbound** command.

- If the settings of the two commands in VTY line view are both the default settings, the settings for the commands in VTY line class view take effect.
- If the settings of the two commands in VTY line view are both non-default settings, the non-default settings in VTY line view take effect.
- If only one command has a non-default setting in VTY line view, the other command uses the default setting, regardless of the setting in VTY line class view.

An authentication mode change does not take effect for the current session. It takes effect for subsequent login sessions.

Examples

Enable the **none** authentication mode for VTY line 0.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] authentication-mode none
```

Enable password authentication for VTY line 0 and set the password to **hello12345**.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] authentication-mode password
[Sysname-line-vty0] set authentication password simple hello12345
```

Enable scheme authentication for VTY line 0. Configure the local user **123** and set the password to **hello12345**. Assign the Telnet service and the user role network-admin to the user.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] authentication-mode scheme
```

```
[Sysname-line-vty0] quit
[Sysname] local-user 123
[Sysname-luser-manage-123] password simple hello12345
[Sysname-luser-manage-123] service-type telnet
[Sysname-luser-manage-123] authorization-attribute user-role network-admin
```

Related commands

set authentication password

auto-execute command

Use **auto-execute command** to specify the command to be automatically executed for a login user.

Use **undo auto-execute command** to restore the default.

Syntax

auto-execute command *command*

undo auto-execute command

Default

No command is specified to be automatically executed for a login user.

Views

User line view

User line class view

Predefined user roles

network-admin

Parameters

command: Specifies the command to be automatically executed.

Usage guidelines

CAUTION:

After configuring this command for a user line, you might be unable to access the CLI through the user line. Make sure you can access the CLI through a different user line before you configure this command and save the configuration.

The device will automatically execute the specified command when a user logs in through the user line, and close the user connection after the command is executed.

This command is not supported in AUX line view or AUX line class view.

This command is available in both user line view and user line class view. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.

A configuration change made by this command does not take effect for the current session. It takes effect for subsequent login sessions.

Examples

Configure the device to automatically execute the **telnet 192.168.1.41** command when a user logs in through VTY line 0.

```
<Sysname> system-view
```

```
[Sysname] line vty 0
[Sysname-line-vty0] auto-execute command telnet 192.168.1.41
This action will lead to configuration failure through line-vty0. Are you sure?
[Y/N]:y
[Sysname-line-vty0]
```

To verify the configuration, Telnet to the device (192.168.1.40).

The device automatically Telnets to 192.168.1.41. The following output is displayed on the configuration terminal:

```
C:\> telnet 192.168.1.40
******************************************************************************
* Copyright (c) 2004-2017 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************


<Sysname>
Trying 192.168.1.41 ...
Press CTRL+K to abort
Connected to 192.168.1.41 ...
******************************************************************************
* Copyright (c) 2004-2017 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************
<Sysname.41>
```

This operation is the same as directly logging in to the device at 192.168.1.41 through Telnet. When you close the Telnet connection to 192.168.1.41, the Telnet connection to 192.168.1.40 is closed at the same time.

command accounting

Use **command accounting** to enable command accounting.

Use **undo command accounting** to disable command accounting.

Syntax

command accounting

undo command accounting

Default

Command accounting is disabled. The accounting server does not record executed commands.

Views

User line view

User line class view

Predefined user roles

network-admin

Usage guidelines

When command accounting is enabled but command authorization is not, every executed command is recorded on the HWTACACS server. When both command accounting and command authorization are enabled, only authorized commands that are executed are recorded on the HWTACACS server.

Invalid commands are not recorded.

A configuration change made by this command does not take effect for the current session. It takes effect for subsequent login sessions.

After you configure the **command accounting** command in user line class view, you cannot configure the **undo command accounting** command in any user line views in the class.

Examples

Enable command accounting for VTY line 0.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] command accounting
```

Related commands

accounting command (*Security Command Reference*)

command authorization

command authorization

Use **command authorization** to enable command authorization.

Use **undo command authorization** to disable command authorization.

Syntax

command authorization

undo command authorization

Default

Command authorization is disabled. Logged-in users can execute commands without authorization.

Views

User line view

User line class view

Predefined user roles

network-admin

Usage guidelines

When command authorization is enabled, a user can only use commands that are permitted by both the AAA scheme and user role.

A configuration change made by this command does not take effect for the current session. It takes effect for subsequent login sessions.

If you configure the **command authorization** command in user line class view, command authorization is enabled for all user lines in the class. You cannot configure the **undo command authorization** command in the view of a user line in the class.

Examples

Enable command authorization for VTY line 0.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] command authorization
```

Related commands

authorization command (*Security Command Reference*)

command accounting

databits

Use **databits** to specify the number of data bits for a character.

Use **undo databits** to restore the default.

Syntax

databits { **5** | **6** | **7** | **8** }

undo databits

Default

Eight data bits are used for a character.

Views

User line view

Predefined user roles

network-admin

Parameters

5: Uses five data bits for a character.

6: Uses six data bits for a character.

7: Uses seven data bits for a character.

8: Uses eight data bits for a character.

Usage guidelines

This command is not supported in VTY line class view.

This setting must be the same as the setting on the configuration terminal.

Examples

Configure AUX 0 to use seven data bits for a character.

```
<Sysname> system-view
[Sysname] line aux 0
[Sysname-line-aux0] databits 7
```

display ip http

Use **display ip http** to display HTTP service configuration and status information.

Syntax

display ip http

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display HTTP service configuration and status information.

```
<Sysname> display ip http
HTTP port: 80
Basic ACL: 2222
Operation status: Enabled
```

Table 2 Command output

Field	Description
HTTP port	HTTP service port number.
Basic ACL	ACL used to control HTTP access. If no ACL is used, this field displays **0**.
Operation status	Whether the HTTP service is enabled.

Related commands

`ip http acl`

`ip http enable`

`ip http port`

display ip https

Use **`display ip https`** to display HTTPS service configuration and status information.

Syntax

`display ip https`

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display HTTPS service configuration and status information.

```
<Sysname> display ip https
HTTPS port: 443
SSL server policy: test
Certificate access control policy: Not configured
Basic ACL: 2222
Operation status: Enabled
```

Table 3 Command output

Field	Description
HTTPS port	HTTPS service port number.

Field	Description
SSL server policy	SSL server policy applied to the HTTPS service. If no SSL server policy is applied, this field displays **Not configured**.
Certificate access-control-policy	Certificate-based access control policy used to control client access rights. If no certificate-based access control policy is used, this field displays **Not configured**.
Basic ACL	ACL used to control HTTPS access. If no ACL is used, this field displays **0**.
Operation status	Whether the HTTPS service is enabled.

Related commands

ip https acl

ip https certificate access-control-policy

ip https enable

ip https port

ip https ssl-server-policy

display line

Use **display line** to display user line information.

Syntax

display line [*number1* | { **aux** | **usb** | **vty** } *number2*] [**summary**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

number1: Specifies the absolute number of a user line. The value range is 0 to 83.

aux: Specifies the AUX line.

usb: Specifies the USB line.

vty: Specifies the VTY line.

number2: Specifies the relative number of a user line. The value range is 0 to 9 for AUX and USB lines and 0 to 63 for VTY lines.

summary: Displays summary information about user lines. If you do not specify this keyword, the command displays detailed information.

Examples

Display information about line 0.

```
<Sysname> display line 0
  Idx  Type     Tx/Rx      Modem Auth  Int        Location
F 0    AUX 0    9600       -     N     -           1/0
```

```
  +    : Line is active.
  F    : Line is active and in async mode.
  Idx  : Absolute index of line.
  Type : Type and relative index of line.
  Auth : Login authentication mode.
  Int  : Physical port of the line.
  A    : Authentication use AAA.
  N    : No authentication is required.
  P    : Password authentication.
```

Table 4 Command output

Field	Description
Modem	Whether the modem allows calling in or out. By default, this attribute is not configured and this field displays a hyphen (-). This field is not supported in the current software version.
Int	Physical port for the line. If there is no physical port for the line or the port is a console port, this field displays a hyphen (-).
Location	Physical position of the line, in the form of *slot number*/*CPU number*.

Display summary information about all user lines.

```
<Sysname> display line summary
  Line type : [AUX]
           0:XXXX XXXX XX
  Line type : [VTY]
          10:UXXX XXXX XXXX XXXX
          26:XXXX XXXX XXXX XXXX
          42:XXXX XXXX XXXX XXXX
          58:XXXX XXXX XXXX XXXX
  Line type : [USB]
          74:XXXX XXXX XX

   1 lines used.      (U)
  83 lines not used.  (X)
```

Table 5 Command output

Fields	Description
Line type	Type of the user line: • **AUX**—AUX line. • **USB**—USB line. • **VTY**—VTY line.
number:*status*	*number*: Absolute number of the first user line in the user line class. *status*: User line status. **X** is for unused and **U** is for used.

display telnet client

Use **`display telnet client`** to display the packet source setting for the Telnet client.

Syntax

display telnet client

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

This command displays the source IPv4 address or source interface specified for the Telnet client to use in outgoing Telnet packets, depending on the **telnet client source** command.

Examples

Display the packet source setting for the Telnet client.

```
<Sysname> display telnet client
 The source IP address is 1.1.1.1.
```

Related commands

telnet client source

display user-interface

Use **display user-interface** to display user line information.

Syntax

display user-interface [*number1* | { **aux** | **usb** | **vty** } *number2*] [**summary**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

number1: Specifies the absolute number of a user line. The value range is 0 to 83.

aux: Specifies the AUX line.

usb: Specifies the USB line.

vty: Specifies the VTY line.

number2: Specifies the relative number of a user line. The value range is 0 to 9 for AUX and USB lines and 0 to 63 for VTY lines.

summary: Displays summary information about user lines. If you do not specify this keyword, the detailed information is displayed.

Usage guidelines

This command is an older version reserved for backward compatibility purposes. It has the same functionality and output as the **display line** command. As a best practice, use the **display line** command.

Examples

Display information about line 0.

```
<Sysname> display user-interface 0
  Idx  Type     Tx/Rx      Modem Auth  Int        Location
F 0    AUX 0    9600       -     N     -          1/0

  +    : Line is active.
  F    : Line is active and in async mode.
  Idx  : Absolute index of line.
  Type : Type and relative index of line.
  Auth : Login authentication mode.
  Int  : Physical port of the line.
  A    : Authentication use AAA.
  N    : No authentication is required.
  P    : Password authentication.
```

Table 6 Command output

Field	Description
Modem	Whether the modem allows calling in or out. By default, this attribute is not configured and this field displays a hyphen (-). This field is not supported in the current software version.
Int	Physical port for the line. If there is no physical port for the line or the port is a console port, this field displays a hyphen (-).
Location	Physical position of the line, in the form of *slot number*/*CPU number*.

Display summary information about all user lines.

```
<Sysname> display user-interface summary
  Line type : [AUX]
            0:XXXX XXXX XX
  Line type : [VTY]
           10:UXXX XXXX XXXX XXXX
           26:XXXX XXXX XXXX XXXX
           42:XXXX XXXX XXXX XXXX
           58:XXXX XXXX XXXX XXXX
  Line type : [USB]
           74:XXXX XXXX XX

   1 lines used.      (U)
  83 lines not used.  (X)
```

Table 7 Command output

Fields	Description
Line type	Type of the user line: • **AUX**—AUX line. • **USB**—USB line. • **VTY**—VTY line.

Fields	Description
number:*status*	*number*: Absolute number of the first user line in the user line class. *status*: User line status. **X** is for unused and **U** is for used.

display users

Use **display users** to display online CLI users.

Syntax

display users [**all**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

all: Displays all user lines supported by the device.

Examples

Display online user information.

```
<Sysname> display users
  Idx  Line     Idle       Time              Pid     Type
+ 10   VTY 0    00:00:00   Jan 01 00:33:10   484     TEL
  12   VTY 2    00:06:22   Jan 01 00:33:22   495     TEL

Following are more details.
VTY 0   :
        User role list: network-admin network-operator
        Location: 192.168.1.107
VTY 2   :
        User role list: level-0 network-admin network-operator
        Location: 192.168.1.134
 +    : Current operation user.
 F    : Current operation user works in async mode.
```

Table 8 Command output

Field	Description
Idx	Absolute number of the user line.
Line	Type and relative number of the user line.
Idle	Time elapsed after the user's most recent input, in the *hh*:*mm*:*ss* format.
Time	Login time of the user.
Pid	Process ID of the user session.

Field	Description
Type	User type: • **TEL**—Telnet user. • **SSH**—SSH user. • For a user who logged in through the console or USB port, this field does not display anything.
+	User line you are using.
User name	Username used by the user. This field is displayed only if the user provided a username and password for authentication at login.
User role list	User roles assigned to the user.
Location	IP address of the user.

display web menu

Use **display web menu** to display Web interface navigation tree information.

Syntax

display web menu [**chinese**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

chinese: Displays information about the Chinese Web interface navigation tree. If you do not specify this keyword, the command displays information about the English Web interface navigation tree.

Usage guidelines

This command displays all options on the Web interface navigation tree.

Examples

Display Web interface navigation tree information.

```
<Sysname> display web menu
.
  |--Dashboard: ID = m_dashboard
  |--Device: ID = m_device
  |    |--Maintenance: ID = m_maintenance
  |    |    |--Settings: ID = m_devicesettings
  |    |    |--Administrators: ID = m_admin
  |    |    |--Configuration: ID = m_config
  |    |    |--File System: ID = m_filesystem
  |    |    |--Upgrade: ID = m_upgrade
  |    |    |--Diagnostics: ID = m_diagnostic
  |    |    |--Reboot: ID = m_reboot
```

```
|    |    `--About: ID = m_about
|    `--Virtualization: ID = m_virtualdevice
|         `--IRF: ID = m_irf
|--Network: ID = m_network
|    |--Probe: ID = m_probe
|    |    |--Ping: ID = m_ping
|    |    `--Tracert: ID = m_tracert
|    |--Interfaces: ID = m_if
|    |    |--Interfaces: ID = m_interface
|    |    |--Link Aggregation: ID = m_lagg
|    |    |--Storm Constrain: ID = m_stormconstrain
|    |    `--Isolation: ID = m_isolation
|    |--Links: ID = m_link
|    |    |--VLAN: ID = m_vlan
|    |    |--Voice VLAN: ID = m_voicevlan
|    |    |--MAC: ID = m_mac
|    |    |--STP: ID = m_stp
|    |    |--LLDP: ID = m_lldp
|    |    `--DHCP Snooping: ID = m_dhcpsnooping
|    |--IP: ID = m_ip
|    |    |--IP: ID = m_ip
|    |    |--ARP: ID = m_arp
|    |    `--DNS: ID = m_dns
|    |--IPv6: ID = m_ipv6
|    |    |--IPv6: ID = m_ipv6
|    |    |--ND: ID = m_nd
|    |    `--DNS: ID = m_ipv6dns
|    |--Mirroring: ID = m_mirror
|    |    `--Port Mirroring: ID = m_portmirror
|    |--Routing: ID = m_routing
|    |    |--Routing Table: ID = m_routingtable
|    |    |--Static Routing: ID = m_staticrouting
|    |    |--RIP: ID = m_rip
|    |    `--Policy-Based Routing: ID = m_pbr
|    |--Multicast: ID = m_multicast
|    |    |--IGMP Snooping: ID = m_igmpsnooping
|    |    `--MLD Snooping: ID = m_mldsnooping
|    `--Service: ID = m_ipservice
|         |--DHCP: ID = m_dhcp
|         |--HTTP/HTTPS: ID = m_http
|         |--SSH: ID = m_ssh
|         |--FTP: ID = m_ftp
|         |--Telnet: ID = m_telnet
|         |--NTP: ID = m_ntp
|         `--SNMP: ID = m_snmp
|--Resources: ID = m_resource
|    |--ACLs: ID = m_acl
|    |    |--IPv4: ID = m_ipv4acl
```

```
|    |    |--IPv6: ID = m_ipv6acl
|    |    `--Ethernet: ID = m_macacl
|    |--Time Range: ID = m_timerange
|    |    `--Time Range: ID = m_timerange
|    |--SSL: ID = m_ssl
|    |    `--SSL: ID = m_ssl
|    |--Public key: ID = m_publickey
|    |    `--Public key: ID = m_publickey
|    `--PKI: ID = m_pki
|         |--PKI: ID = m_pki
|         `--Certificate Access Control: ID = m_certificatepolicy
|--QoS: ID = m_qos
|    `--QoS: ID = m_qos
|         |--QoS Policies: ID = m_mqc
|         |--Hardware Queuing: ID = m_hardqueue
|         |--Priority Mapping: ID = m_priority
|         `--Rate Limit: ID = m_linerate
|--Security: ID = m_security
|    |--Packet Filter: ID = m_packetfilter
|    |    |--Packet Filter: ID = m_packetfilter
|    |    `--IP Source Guard: ID = m_ipsourceguard
|    |--Access Control: ID = m_access
|    |    |--802.1X: ID = m_8021x
|    |    |--MAC Authentication: ID = m_maca
|    |    |--Port Security: ID = m_portsec
|    |    `--Portal: ID = m_portal
|    `--Authentication: ID = m_authentication
|         |--ISP Domains: ID = m_ispdomain
|         |--RADIUS: ID = m_radius
|         |--TACACS: ID = m_tacacs
|         `--Local Users: ID = m_localuser
|--PoE: ID = m_poe
|    `--PoE: ID = m_poe
|         `--PoE: ID = m_poe
|--SmartMC: ID = m_smartmc
`--Log: ID = m_log
     `--Log: ID = m_log
          |--System Log: ID = m_syslog
          `--Settings: ID = m_logsettings
```

display web users

Use **display web users** to display online Web users.

Syntax

display web users

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display online Web users.

```
<Sysname> display web users
UserID          Name            Type   Language JobCount LoginTime LastOperation
AB2039483271293 Administrator   HTTP   Chinese     3     12:00:23  14:10:05
F09382BA2014AC8 user            HTTPS  English     1     13:05:00  14:11:00
```

Table 9 Command output

Field	Description
UserID	ID used to uniquely identify the online Web user.
JobCount	Number of connections established by the user.

escape-key

Use **escape-key** to set the escape key.

Use **undo escape-key** to disable the escape key.

Syntax

escape-key { *key-string* | **default** }

undo escape-key

Default

The escape key is **Ctrl+C**.

Views

User line view

User line class view

Predefined user roles

network-admin

Parameters

key-string: Specifies a shortcut key. It can be a character (case sensitive, except for **d** and **D**), or an ASCII code value in the range of 0 to 127. For example, if you configure **escape-key 1**, the shortcut key is **Ctrl+A**. If you configure **escape-key a**, the shortcut key is **a**. If you specify the character **d** or **D** for this argument, the actual shortcut key is **Ctrl+C**. To use **d** or **D** as the shortcut key, you must specify the ASCII code value of the character for this argument. For information about ASCII code values of individual characters, see the standard ASCII code chart. For information about ASCII code values of combined keys that use the **Ctrl** key, see Table 1.

default: Restores the default escape key **Ctrl+C**.

Usage guidelines

You can press the escape key to abort a command that is being executed, for example, a **ping** or **tracert** command. Whether a command can be aborted by **Ctrl+C** by default depends on the

software implementation of the command. For more information, see the usage guidelines for the command.

As a best practice, use a key sequence as the escape key. If you define a single character as the escape key, pressing the key while a command is being executed stops the command. If no command is being executed, pressing the key enters the character as a common character. If you Telnet from the device to a remote device, pressing the key enters the character as a common character on the remote device. The key acts as the escape key on the remote device only when the following conditions are met:

- You define the same character as the escape key on the remote device.
- You press the key while a command is being executed on the remote device.

The **undo escape-key** command disables the current escape key. After you execute this **undo** command, no escape key is available.

This command is available in both user line view and user line class view. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.

The setting in user line view takes effect immediately for the current session. The setting in user line class view takes effect for login sessions that are established after the setting is configured.

To display the current escape key, use the **display current-configuration | include escape-key** command.

Examples

Configure character **a** as the escape key for VTY line 0.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] escape-key a
```

To verify the configuration:

1. Ping IP address 192.168.1.80, specifying the **-c** keyword to set the number of ICMP echo request packets to 20.

   ```
   <Sysname> ping -c 20 192.168.1.80
   Ping 192.168.1.80 (192.168.1.80): 56 data bytes, press 'a' to break
   56 bytes from 192.168.1.80: icmp_seq=0 ttl=255 time=2.363 ms
   56 bytes from 192.168.1.80: icmp_seq=1 ttl=255 time=2.384 ms
   ```

2. Press **a**.

   The system aborts the command and returns to user view.

   ```
   --- Ping statistics for 192.168.1.80 ---
   20 packet(s) transmitted, 20 packet(s) received, 0.0% packet loss
   round-trip min/avg/max/std-dev = 2.000/2.406/6.748/1.022 ms
   <Sysname>
   ```

flow-control

Use **flow-control** to configure the flow control mode.

Use **undo flow-control** to restore the default.

Syntax

flow-control { **hardware** | **none** | **software** }

undo flow-control

Default

Flow control is disabled.

Views

User line view

Predefined user roles

network-admin

Parameters

hardware: Performs hardware flow control.

none: Disables flow control.

software: Performs software flow control.

Usage guidelines

This command is not supported in VTY line view.

The device supports flow control in both the inbound and outbound directions.

- For flow control in the inbound direction, the local device listens to flow control information from the remote device.
- For flow control in the outbound direction, the local device sends flow control information to the remote device.

The flow control setting takes effect in both directions.

To communicate, two devices must operate in the same flow control mode.

Examples

Configure software flow control in the inbound and outbound directions for AUX line 0.

```
<Sysname> system-view
[Sysname] line aux 0
[Sysname-line-aux0] flow-control software
```

free line

Use **free line** to release a user line.

Syntax

free line { *number1* | { **aux** | **usb** | **vty** } *number2* }

Views

User view

Predefined user roles

network-admin

Parameters

number1: Specifies the absolute number of a user line. The value range is 0 to 83.

aux: Specifies the AUX line.

usb: Specifies the USB line.

vty: Specifies the VTY line.

number2: Specifies the relative number of a user line. The value range is 0 to 9 for AUX and USB lines and 0 to 63 for VTY lines.

Usage guidelines

This command does not release the line you are using.

Examples

Release VTY line 1.

```
<Sysname> free line vty 1
Are you sure to free line vty1? [Y/N]:y
 [OK]
```

free user-interface

Use **free user-interface** to release a user line.

Syntax

free user-interface { *number1* | { **aux** | **usb** | **vty** } *number2* }

Views

User view

Predefined user roles

network-admin

Parameters

number1: Specifies the absolute number of a user line. The value range is 0 to 83.

aux: Specifies the AUX line.

usb: Specifies the USB line.

vty: Specifies the VTY line.

number2: Specifies the relative number of a user line. The value range is 0 to 9 for AUX and USB lines and 0 to 63 for VTY lines.

Usage guidelines

This command does not release the line you are using.

This command is an older version reserved for backward compatibility purposes. It has the same functionality and output as the **free line** command. As a best practice, use the **free line** command.

Examples

Release VTY line 1.

```
<Sysname> free user-interface vty 1
Are you sure to free line vty1? [Y/N]:y
 [OK]
```

free web users

Use **free web users** to log off online Web users.

Syntax

free web users { **all** | **user-id** *user-id* | **user-name** *user-name* }

Views

User view

Predefined user roles

network-admin

Parameters

all: Specifies all Web users.

user-id: Specifies a Web user by the ID, a hexadecimal number of 15 digits. The system assigns each Web user a unique ID at login to identify the user.

user-name: Specifies a Web user by the username, a case-sensitive string of 1 to 255 characters.

Examples

Log off all online Web users.

```
<Sysname> free web users all
```

Related commands

display web users

history-command max-size

Use **history-command max-size** to set the size of the command history buffer for a user line.

Use **undo history-command max-size** to restore the default.

Syntax

history-command max-size *size-value*

undo history-command max-size

Default

The command history buffer for a user line stores up to 10 history commands.

Views

User line view

User line class view

Predefined user roles

network-admin

Parameters

size-value: Specifies the maximum number of history commands the buffer can store, in the range of 0 to 256.

Usage guidelines

Each user line uses a separate command history buffer to store commands successfully executed by its user. The buffer size determines how many history commands the buffer can store.

To display history commands in the buffer for your session, press the up or down arrow key, or execute the **display history-command** command. For more information about the command history buffer, see *Fundamentals Configuration Guide*.

Terminating a CLI session clears the commands in the command history buffer.

The setting in user line view takes effect immediately for the current session. The setting in user line class view takes effect for login sessions that are established after the setting is configured.

Examples

Set the command history buffer size to 20 for VTY line 0.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] history-command max-size 20
```

idle-timeout

Use **idle-timeout** to set the CLI connection idle-timeout timer.

Use **undo idle-timeout** to restore the default.

Syntax

idle-timeout *minutes* [*seconds*]

undo idle-timeout

Default

The CLI connection idle-timeout timer is 10 minutes.

Views

User line view

User line class view

Predefined user roles

network-admin

Parameters

minutes: Specifies the number of minutes, in the range of 0 to 35791.

seconds: Specifies the number of seconds, in the range of 0 to 59. The default is 0 seconds.

Usage guidelines

The system automatically terminates a user connection if no information interaction occurs on the connection within the idle-timeout interval.

To disable the idle-timeout feature, execute the **idle-timeout 0** command.

This command is available in both user line view and user line class view. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.

The setting in user line view takes effect immediately for the current session. The setting in user line class view takes effect for login sessions that are established after the setting is configured.

Examples

Set the CLI connection idle-timeout timer to 1 minute and 30 seconds for VTY line 0.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] idle-timeout 1 30
```

ip http acl

Use **ip http acl** to apply an ACL to the HTTP service.

Use **undo ip http acl** to restore the default.

Syntax

ip http acl { *acl-number* | **name** *acl-name* }

undo ip http acl

Default

No ACL is applied to the HTTP service.

Views

System view

Predefined user roles

network-admin

Parameters

acl-number: Specifies an ACL by its number. The value range is 2000 to 2999.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters. It must start with an English letter and to avoid confusion, it cannot be **all**. The specified ACL takes effect only when the ACL exists and is a basic ACL.

Usage guidelines

This command is not supported in FIPS mode.

If you execute this command multiple times, the most recent configuration takes effect.

Only clients permitted by the applied ACL can access the device through HTTP.

Examples

Use ACL 2001 to allow only users from 10.10.0.0/16 to access the device through HTTP.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] ip http acl 2001
```

Related commands

acl (*ACL and QoS Command Reference*)

ip http enable

Use **ip http enable** to enable the HTTP service.

Use **undo ip http enable** to disable the HTTP service.

Syntax

ip http enable

undo ip http enable

Default

On the S5000V3-EI, S5000V5-EI, S5000E-X, S5000X-EI, WS5810-WiNet, WS5820-WiNet, and WAS6000 switch series, the default setting varies by startup configuration.

- If the device starts up with factory defaults, the HTTP service is enabled.
- If the device starts up with the initial configuration, the HTTP service is disabled.

On the other switch series, the HTTP service is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command is not supported in FIPS mode.

To allow users to access the device through HTTP, you must enable the HTTP service.

To improve device security, the system automatically enables the HTTPS service when you enable the HTTP service. When the HTTP service is enabled, you cannot disable the HTTPS service.

Examples

Enable the HTTP service.

```
<Sysname> system-view
[Sysname] ip http enable
```

Related commands

ip https enable

ip http port

Use **ip http port** to specify the HTTP service port number.

Use **undo ip http port** to restore the default.

Syntax

ip http port *port-number*

undo ip http port

Default

The HTTP service port number is 80.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies a port number in the range of 1 to 65535.

Usage guidelines

This command is not supported in FIPS mode.

When the HTTP service is enabled, changing the HTTP service port number re-enables the HTTP service and closes all HTTP connections. To log in again, users must enter the new URL in the Web browser's address bar.

Examples

Set the HTTP service port number to 80.

```
<Sysname> system-view
[Sysname] ip http port 80
```

ip https acl

Use **ip https acl** to apply an ACL to the HTTPS service.

Use **undo ip https acl** to restore the default.

Syntax

ip https acl { *acl-number* | **name** *acl-name* }

undo ip https acl

Default

No ACL is applied to the HTTP service.

Views

System view

Predefined user roles

network-admin

Parameters

acl-number: Specifies an ACL by its number. The value range is 2000 to 2999.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters. It must start with an English letter and to avoid confusion, it cannot be **all**. The specified ACL takes effect only when the ACL exists and is a basic ACL.

Usage guidelines

To access the device, HTTPS clients must be permitted by the ACL applied to the HTTPS service.

Because the device always uses HTTPS to transfer Web login requests, the ACL applied to the HTTPS service controls both HTTPS and HTTP logins. To access the device, HTTP clients must be permitted by the following ACLs:

- ACL applied to the HTTP service.
- ACL applied to the HTTPS service.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Use ACL 2001 to allow only users from 10.10.0.0/16 to access the device through HTTPS or HTTP.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] ip https acl 2001
```

Related commands

acl (*ACL and QoS Command Reference*)

ip https certificate access-control-policy

Use **ip https certificate access-control-policy** to apply a certificate-based access control policy to control HTTPS access.

Use **undo ip https certificate access-control-policy** to restore the default.

Syntax

ip https certificate access-control-policy *policy-name*

undo ip https certificate access-control-policy

Default

No certificate-based access control policy is applied for HTTPS access control.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a certificate-based access control policy by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

For more information about the certificate-based access control policy, see PKI configuration in *Security Configuration Guide*.

Examples

Use certificate-based access control policy **myacl** to control HTTPS access.

```
<Sysname> system-view
[Sysname] ip https certificate access-control-policy myacl
```

Related commands

pki certificate access-control-policy (*Security Command Reference*)

ip https enable

Use **ip https enable** to enable the HTTPS service.

Use **undo ip https enable** to disable the HTTPS service.

Syntax

ip https enable

undo ip https enable

Default

On the S5000V3-EI, S5000V5-EI, S5000E-X, S5000X-EI, WS5810-WiNet, WS5820-WiNet, and WAS6000 switch series, the default setting varies by startup configuration.

- If the device starts up with factory defaults, the HTTPS service is enabled.
- If the device starts up with the initial configuration, the HTTPS service is disabled.

On the other switch series, the HTTPS service is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

To allow users to access the device through HTTPS, you must enable the HTTPS service.

Enabling the HTTPS service triggers the SSL handshake negotiation process.

- If the device has a local certificate, the SSL handshake negotiation succeeds and the HTTPS service starts up.

- If the device does not have a local certificate, the certificate application process starts. Because the certificate application process takes a long time, the SSL handshake negotiation might fail and the HTTPS service might not be started. To solve the problem, execute this command again until the HTTPS service is enabled.

Examples

Enable the HTTPS service.

```
<Sysname> system-view
[Sysname] ip https enable
```

Related commands

ip https certificate access-control-policy

ip https ssl-server-policy

ip https port

Use **ip https port** to specify the HTTPS service port number.

Use **undo ip https port** to restore the default.

Syntax

ip https port *port-number*

undo ip https port

Default

The HTTPS service port number is 443.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies a port number in the range of 1 to 65535.

Usage guidelines

When the HTTPS service is enabled, changing the HTTPS service port number re-enables the HTTPS service and closes all HTTPS and HTTP connections. To log in again, users must enter the new URL in the Web browser's address bar.

Examples

Set the HTTPS service port number to 8080.

```
<Sysname> system-view
[Sysname] ip https port 8080
```

ip https ssl-server-policy

Use **ip https ssl-server-policy** to apply an SSL server policy to control HTTPS access.

Use **undo ip https ssl-server-policy** to restore the default.

Syntax

ip https ssl-server-policy *policy-name*

undo ip https ssl-server-policy

Default

No SSL server policy is applied. The HTTPS service uses a self-signed certificate.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies an SSL server policy name, a string of 1 to 31 characters.

Usage guidelines

If the HTTP service and HTTPS service are enabled, changes to the applied SSL server policy do not take effect. For the changes to take effect, you must disable HTTP and HTTPS, and then apply the policy and enable HTTP and HTTPS again.

To restore the default, you must disable HTTP and HTTPS, execute the **undo ip https ssl-server-policy** command, and then enable HTTP and HTTPS again.

Examples

Apply SSL server policy **myssl** to the HTTPS service.

```
<Sysname> system-view
[Sysname] ip https ssl-server-policy myssl
```

Related commands

ssl server-policy (*Security Command Reference*)

line

Use **line** to enter one or multiple user line views.

Syntax

line { *first-number1* [*last-number1*] | { **aux** | **usb** | **vty** } *first-number2* [*last-number2*] }

Views

System view

Predefined user roles

network-admin

Parameters

first-number1: Specifies the absolute number of the first user line. The value range is 0 to 83.

last-number1: Specifies the absolute number of the last user line. The value range is 1 to 83. This number must be greater than *first-number1*.

aux: Specifies the AUX line.

usb: Specifies the USB line.

vty: Specifies the VTY line.

first-number2: Specifies the relative number of the first user line. The value range is 0 to 9 for AUX and USB lines and 0 to 63 for VTY lines.

last-number2: Specifies the relative number of the last user line. The value range is 1 to 9 for AUX and USB lines and 1 to 63 for VTY lines. This number must be greater than *first-number2*.

Examples

Enter the view of VTY line 0.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0]
```

Enter the views of VTY lines 0 to 63.

```
<Sysname> system-view
[Sysname] line vty 0 63
[Sysname-line-vty0-63]
```

Related commands

line class

line class

Use **line class** to enter user line class view.

Syntax

line class { **aux** | **usb** | **vty** }

Views

System view

Predefined user roles

network-admin

Parameters

aux: Specifies the AUX line class view.

usb: Specifies the USB line.

vty: Specifies the VTY line class view.

Usage guidelines

To configure the same settings for all user lines of a line class, use this command to enter the user line class view.

In user line class view, you can execute the following commands:

- **activation-key**
- **auto-execute command**
- **authentication-mode**
- **command accounting**
- **command authorization**
- **escape-key**
- **history-command max-size**
- **idle-timeout**
- **protocol inbound**
- **screen-length**

- **set authentication password**
- **shell**
- **terminal type**
- **user-role**

For commands that are available in both user line view and user line class view, the device uses the following rules to determine the settings to use:

- A setting in user line view applies only to the user line. A setting in user line class view applies to all user lines of the class.
- A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.
- A setting in user line class view does not take effect for current online users. It takes effect only for new login users.

Examples

Set the CLI connection idle-timeout timer to 15 minutes in VTY line class view.

```
<Sysname> system-view
[Sysname] line class vty
[Sysname-line-class-vty] idle-timeout 15
```

In AUX line class view, configure the character **s** as the terminal session activation key.

```
<Sysname> system-view
[Sysname] line class aux
[Sysname-line-class-aux] activation-key s
[Sysname-line-class-aux] quit
```

In the view of AUX line 0, restore the default terminal session activation key.

```
[Sysname] line aux 0
[Sysname-line-aux0] undo activation-key
```

Alternatively, you can use the following command:

```
[Sysname-line-aux0] activation-key 13
```

To verify the configuration:

1. Exit the session on AUX line 0.

   ```
   [Sysname-line-aux0] return
   <Sysname> quit
   ```

2. Log in again through the user line.

   The following message appears:

   ```
   Press ENTER to get started.
   ```

3. Press **Enter**.

   Pressing **Enter** does not start a session.

4. Enter **s**.

   A terminal session is started.

   ```
   <Sysname>
   ```

Related commands

line

lock

Use **lock** to lock the current user line and set the password for unlocking the line.

Syntax

lock

Default

The system does not lock any user lines.

Views

User view

Predefined user roles

network-admin

Usage guidelines

This command is not supported in FIPS mode.

This command locks the current user line to prevent unauthorized users from using the line. You must set the password for unlocking the line as prompted. The user line is locked after you enter the password and confirm the password.

To unlock the user line, press **Enter** and enter the password you set.

Examples

Lock the current user line and set the password for unlocking the line.

```
<Sysname> lock
Please input password<1 to 16> to lock current line:
Password:
Again:

                    locked !
```

// The user line is locked. To unlock it, press **Enter** and enter the password:

```
Password:
<Sysname>
```

lock reauthentication

Use **lock reauthentication** to lock the current user line and enable unlocking authentication.

Syntax

lock reauthentication

Default

The system does not lock any user lines or initiate reauthentication.

Views

Any view

Predefined user roles

network-admin

Usage guidelines

This command locks the current user line. To unlock the user line, you must press **Enter** and provide the login password to pass reauthentication. If you have changed the login password after login, you must provide the new password. If no login password is set, the system unlocks the user line after you press **Enter**.

Examples

Lock the current user line and enable unlocking authentication.

```
<Sysname> lock reauthentication

Please press Enter to unlock the screen.
```

// The user line is locked. To unlock it, press **Enter** and enter the login password:

```
Password:

<Sysname>
```

Related commands

lock-key

lock-key

Use **lock-key** to set the user line locking key. Pressing this shortcut key locks the current user line and enables unlocking authentication.

Use **undo lock-key** to restore the default.

Syntax

lock-key *key-string*

undo lock-key

Default

No user line locking key is set.

Views

User line view

User line class view

Predefined user roles

network-admin

Parameters

key-string: Specifies a shortcut key. It can be a character (case sensitive), or an ASCII code value in the range of 0 to 127. For example, if you configure **lock-key 1**, the shortcut key is **Ctrl+A**. If you configure **lock-key a**, the shortcut key is **a**. For information about ASCII code values of individual characters, see the standard ASCII code chart. For information about ASCII code values of combined keys that use the **Ctrl** key, see Table 1.

Usage guidelines

As a best practice, specify a combined key as the user line locking key. If you specify a single character as the key, the character acts only as the user line locking key. You cannot type the character for any commands, keywords, or arguments.

Pressing the user line locking key is equivalent to executing the **lock reauthentication** command.

This command takes effect immediately.

To display the current user line locking key, use the **display current-configuration | include lock-key** command.

Examples

Set the user line locking key to **Ctrl+A** for VTY line 0.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] lock-key 1
[Sysname-line-vty0] quit
```

To verify the configuration:

1. Press **Ctrl+A**.

```
[Sysname]

Please press Enter to unlock the screen.
```

2. Press **Enter** and enter the login password.

```
Password:

[Sysname]
```

Related commands

lock reauthentication

parity

Use **parity** to specify the parity.

Use **undo parity** to restore the default.

Syntax

parity { **even** | **mark** | **none** | **odd** | **space** }

undo parity

Default

The setting is **none**. No parity is used.

Views

User line view

Predefined user roles

network-admin

Parameters

even: Uses even parity.

mark: Uses mark parity.

none: Uses no parity.

odd: Uses odd parity.

space: Uses space parity.

Usage guidelines

This command is not supported in VTY line view.

The configuration terminal and the device must use the same parity.

Examples

Configure AUX line 0 to use odd parity.

```
<Sysname> system-view
[Sysname] line aux 0
[Sysname-line-aux0] parity odd
```

protocol inbound

Use **protocol inbound** to specify the supported protocols.

Use **undo protocol inbound** to restore the default.

Syntax

In non-FIPS mode:

protocol inbound { **all** | **ssh** | **telnet** }

undo protocol inbound

In FIPS mode:

protocol inbound ssh

undo protocol inbound

Default

In non-FIPS mode, both protocols are supported.

In FIPS mode, SSH is supported.

Views

VTY line view

VTY line class view

Predefined user roles

network-admin

Parameters

all: Supports both SSH and Telnet protocols.

ssh: Supports SSH only.

telnet: Supports Telnet only.

Usage guidelines

Only users assigned the network-admin, or level-15 user role can execute this command. Other users cannot execute this command, even if they are granted the right to execute this command.

A configuration change in user line view does not take effect for the current session. It takes effect for subsequent login sessions.

Before configuring a user line to support SSH, set the authentication mode to **scheme** for the user line.

In VTY line view, this command is associated with the **authentication-mode** command. If you specify a non-default value for one of the two commands, the other command uses the default setting, regardless of the setting in VTY line class view.

- If the settings of the two commands in VTY line view are both the default settings, the settings for the commands in VTY line class view take effect.
- If the settings of the two commands in VTY line view are both non-default settings, the non-default settings in VTY line view take effect.
- If only one command has a non-default setting in VTY line view, the other command uses the default setting, regardless of the setting in VTY line class view.

Examples

Enable user lines VTY 0 through VTY 4 to support only SSH.

```
<Sysname> system-view
[Sysname] line vty 0 4
[Sysname-line-vty0-4] authentication-mode scheme
[Sysname-line-vty0-4] protocol inbound ssh
```

Enable SSH support and set the authentication mode to scheme in VTY line class view. Enable user lines VTY 0 through VTY 4 to support all protocols and disable authentication for the user lines.

```
<Sysname> system-view
[Sysname] line class vty
[Sysname-line-class-vty] authentication-mode scheme
[Sysname-line-class-vty] protocol inbound ssh
[Sysname-line-class-vty] line vty 0 4
[Sysname-line-vty0-4] authentication-mode none
```

To verify the configuration:

1. Telnet to the device.

```
<Client> telnet 192.168.1.241
Trying 192.168.1.241 ...
Press CTRL+K to abort
Connected to 192.168.1.241 ...

******************************************************************************
* Copyright (c) 2004-2017 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************


<Server>
```

You are logged in without authentication.

2. Display online CLI user information.

```
<Server> display users
  Idx  Line     Idle       Time              Pid     Type
+ 50   VTY 0    00:00:00   Jan 17 15:29:27   189     TEL

Following are more details.
VTY 0   :
        User role list: network-admin network-operator
        Location: 192.168.1.186
 +    : Current operation user.
```

```
F    : Current operation user works in async mode.
```

The output shows that you are using VTY 0. The configuration in user line view is effective.

Related commands

authentication-mode

restful http enable

Use **restful http enable** to enable RESTful access over HTTP.

Use **undo restful http enable** to disable RESTful access over HTTP.

Syntax

restful http enable

undo restful http enable

Default

RESTful access over HTTP is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command is not supported in FIPS mode.

For users to access the device through the HTTP-based RESTful API, you must enable RESTful access over HTTP.

Examples

Enable RESTful access over HTTP.

```
<Sysname> system-view
[Sysname] restful http enable
```

restful https enable

Use **restful https enable** to enable RESTful access over HTTPS.

Use **undo restful https enable** to disable RESTful access over HTTPS.

Syntax

restful https enable

undo restful https enable

Default

RESTful access over HTTPS is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

For users to access the device through the HTTPS-based RESTful API, you must enable RESTful access over HTTPS.

Examples

Enable RESTful access over HTTPS.

```
<Sysname> system-view
[Sysname] restful https enable
```

screen-length

Use **screen-length** to set the maximum number of lines of command output to send to the terminal at a time when the screen pausing feature is enabled.

Use **undo screen-length** to restore the default.

Syntax

screen-length *screen-length*

undo screen-length

Default

A maximum of 24 lines are sent.

Views

User line view

User line class view

Predefined user roles

network-admin

Parameters

screen-length: Specifies the maximum number of lines to send, in the range of 0 to 512. To send command output without pausing, set the number to 0 or execute the **screen-length disable** command.

Usage guidelines

The number of lines that can be displayed on the terminal screen is restricted by both this setting and the display specification of the terminal. For example, if this setting is 40, the device sends 40 lines to the terminal at a time. If the terminal display specification is 24 lines, only the last 24 lines are displayed on the terminal screen. To view the previous 16 lines, you must press **PgUp**.

To continue to display command output after a pause, press the space bar.

By default, pausing between screens of output is enabled.

This command is available in both user line view and user line class view. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.

The setting in user line view takes effect immediately for the current session. The setting in user line class view takes effect for login sessions that are established after the setting is configured.

Examples

Set the maximum number of lines to send at a time to 30 for VTY line 0.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] screen-length 30
```

Related commands

screen-length disable

send

Use **send** to send messages to online login users.

Syntax

send { **all** | *number1* | { **aux** | **usb** | **vty** } *number2* }

Views

User view

Predefined user roles

network-admin

Parameters

all: Specifies all user lines.

number1: Specifies the absolute number of a user line. The value range is 0 to 83.

aux: Specifies the AUX line.

usb: Specifies the USB line.

vty: Specifies the VTY line.

number2: Specifies the relative number of a user line. The value range is 0 to 9 for AUX and USB lines and 0 to 63 for VTY lines.

Usage guidelines

You can use this command to send notifications to online users before performing an operation that might affect other online users, for example, before rebooting the device.

To end a message, press **Enter**. To abort the send operation, press **Ctrl+C**.

Examples

Send a notification to the user on VTY 1.

```
<Sysname> send vty 1
Input message, end with Enter; abort with CTRL+C:
Your attention, please. I will reboot the system in 3 minutes.
Send message? [Y/N]:y
```

The message should appear on the user's terminal screen as follows:

```
[Sysname]


***
***
***Message from vty0 to vty1
***
Your attention, please. I will reboot the system in 3 minutes.
```

set authentication password

Use **set authentication password** to set the password for local password authentication.

Use **undo set authentication password** to restore the default.

Syntax

set authentication password { **hash** | **simple** } *string*

undo set authentication password

Default

No password is set for local password authentication.

Views

User line view

User line class view

Predefined user roles

network-admin

Parameters

hash: Specifies a password in hashed form.

simple: Sets a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in hashed form.

string: Specifies the password. Its hashed form is a case-sensitive string of 1 to 110 characters. In versions earlier than Release 6318P01, its plaintext form is a case-sensitive string of 1 to 16 characters. In Release 6318P01 and later, its plaintext form is a case-sensitive string of 4 to 16 characters, and must contain a minimum of two character types.

Usage guidelines

This command is not supported in FIPS mode.

Only users assigned the network-admin, or level-15 user role can execute this command. Other users cannot execute this command, even if they are granted the right to execute this command.

This command is available in both user line view and user line class view. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.

A password change does not take effect for the current session. It takes effect for subsequent login sessions.

Examples

Set the password to **hello12345** for local password authentication on VTY line 0.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] authentication-mode password
[Sysname-line-vty0] set authentication password simple hello12345
```

Related commands

authentication-mode

shell

Use **shell** to enable the terminal service for user lines.

Use **undo shell** to disable the terminal service for user lines.

Syntax

shell

undo shell

Default

The terminal service is enabled on all user lines.

Views

User line view

User line class view

Predefined user roles

network-admin

Usage guidelines

The **undo shell** command is not supported in AUX line view or AUX line class view.

You cannot disable the terminal service on the user line you are using.

When the device acts as a Telnet or SSH server, you cannot configure the **undo shell** command.

If the **undo shell** command is configured in user line class view, you cannot configure the **shell** command in the view of a user line in the class.

Examples

Disable the terminal service for VTY lines VTY 0 through 4 so no user can log in to the device through the user lines.

```
<Sysname> system-view
[Sysname] line vty 0 4
[Sysname-line-vty0-4] undo shell
Disable ui-vty0-4 , are you sure? [Y/N]:y
[Sysname-line-vty0-4]
```

speed

Use **speed** to set the transmission rate (also called the baud rate) on a user line.

Use **undo speed** to restore the default.

Syntax

speed *speed-value*

undo speed

Default

The transmission rate is 9600 bps on a user line.

Views

User line view

Predefined user roles

network-admin

Parameters

speed-value: Specifies the transmission rate in bps. Supported transmission rates depend on the network environment. The transmission rates for asynchronous serial interfaces might include:

- 300 bps.
- 600 bps.
- 1200 bps.

- 2400 bps.
- 4800 bps.
- 9600 bps.
- 19200 bps.
- 38400 bps.
- 57600 bps.
- 115200 bps.

Usage guidelines

This command is not supported in VTY line view.

The configuration terminal and the device must be configured with the same transmission rate to communicate.

Examples

Set the transmission rate to 19200 bps for AUX line 0.

```
<Sysname> system-view
[Sysname] line aux 0
[Sysname-line-aux0] speed 19200
```

stopbits

Use **stopbits** to specify the number of stop bits for a character.

Use **undo stopbits** to restore the default.

Syntax

stopbits { **1** | **1.5** | **2** }

undo stopbits

Default

One stop bit is used.

Views

User line view

Predefined user roles

network-admin

Parameters

1: Uses one stop bit.

1.5: Uses one and a half stop bits. The device does not support using one and a half stop bits. If you specify this keyword, two stop bits are used.

2: Uses two stop bits.

Usage guidelines

This command is not supported in VTY line view.

The configuration terminal and the device must use the same number of stop bits to communicate.

Examples

Set the number of stop bits to 1 for AUX line 0.

```
<Sysname> system-view
```

```
[Sysname] line aux 0
[Sysname-line-aux0] stopbits 1
```

telnet

Use **telnet** to Telnet to a host in an IPv4 network.

Syntax

telnet *remote-host* [*service-port*] [**source** { **interface** *interface-type interface-number* | **ip** *ip-address* } | **dscp** *dscp-value*] *

Views

User view

Predefined user roles

network-admin

Parameters

remote-host: Specifies the IPv4 address or host name of a remote host. A host name can be a case-insensitive string of 1 to 253 characters. Valid characters include letters, digits, hyphens (-), underscores (_), and dots (.).

service-port: Specifies the TCP port number for the Telnet service on the remote host. The value range is 0 to 65535 and the default is 23.

source: Specifies a source IPv4 address or source interface for outgoing Telnet packets. If you do not specify this option, the device uses the primary IPv4 address of the output interface for the route to the server as the source address.

interface *interface-type interface-number*: Specifies the source interface. The primary IPv4 address of the interface will be used as the source IPv4 address for outgoing Telnet packets.

ip *ip-address*: Specifies the source IPv4 address for outgoing Telnet packets.

dscp *dscp-value*: Specifies a DSCP value for outgoing Telnet packets. The value range is 0 to 63. The default is 48.

Usage guidelines

This command is not supported in FIPS mode.

To terminate the current Telnet connection, press **Ctrl+K** or execute the **quit** command.

The source address or interface specified by this command is applied only to the Telnet connection that is being established.

Examples

Telnet to host 1.1.1.2, using 1.1.1.1 as the source IP address for outgoing Telnet packets.

```
<Sysname> telnet 1.1.1.2 source ip 1.1.1.1
```

Related commands

telnet client source

telnet client source

Use **telnet client source** to specify a source IPv4 address or source interface for the Telnet client to use for outgoing Telnet packets.

Use **undo telnet client source** to restore the default.

Syntax

telnet client source { **interface** *interface-type interface-number* | **ip** *ip-address* }

undo telnet client source

Default

No source IPv4 address or source interface is specified. The Telnet client uses the primary IPv4 address of the output interface for the route to the server as the source IPv4 address.

Views

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a source interface. The primary IPv4 address of the interface will be used as the source IPv4 address for outgoing Telnet packets.

ip *ip-address*: Specifies a source IPv4 address.

Usage guidelines

This command is not supported in FIPS mode.

The setting configured by this command applies to all Telnet connections but has a lower precedence than the source setting specified for the **telnet** command.

Examples

Set the source IPv4 address to 1.1.1.1 for outgoing Telnet packets.

```
<Sysname> system-view
[Sysname] telnet client source ip 1.1.1.1
```

Related commands

display telnet client configuration

telnet ipv6

Use **telnet ipv6** to Telnet to a host in an IPv6 network.

Syntax

telnet ipv6 *remote-host* [**-i** *interface-type interface-number*] [*port-number*] [**source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* } | **dscp** *dscp-value*] *

Views

User view

Predefined user roles

network-admin

Parameters

remote-host: Specifies the IPv6 address or host name of a remote host. A host name can be a case-insensitive string of 1 to 253 characters. Valid characters include letters, digits, hyphens (-), underscores (_), and dots (.).

-i *interface-type interface-number*: Specifies the interface for sending Telnet packets. This option is required when the remote host address is a link-local address. When the server address is a global unicast address, you cannot specify this option.

port-number: Specifies the TCP port number for the Telnet service on the remote host. The value range is 0 to 65535 and the default is 23.

source: Specifies a source IPv6 address or source interface for outgoing Telnet packets. If you do not specify this option, the device uses the primary IPv6 address of the output interface for the route to the server as the source address.

interface *interface-type interface-number*: Specifies the source interface. The primary IPv6 address of the interface will be used as the source IPv6 address for outgoing Telnet packets.

ipv6 *ipv6-address*: Specifies the source IPv6 address for outgoing Telnet packets.

dscp *dscp-value*: Specifies a DSCP value for outgoing Telnet packets. The value range is 0 to 63. The default is 48.

Usage guidelines

This command is not supported in FIPS mode.

To terminate the current Telnet connection, press **Ctrl+K** or execute the **quit** command.

Examples

Telnet to the host at 5000::1.

```
<Sysname> telnet ipv6 5000::1
```

Telnet to the host at 2000::1. Use 1000::1 as the source address for outgoing Telnet packets.

```
<Sysname> telnet ipv6 2000::1 source ipv6 1000::1
```

telnet server acl

Use **telnet server acl** to apply an ACL to filter Telnet logins.

Use **undo telnet server acl** to restore the default.

Syntax

telnet server acl [**mac**] *acl-number*

undo telnet server acl

Default

No ACL is used to filter Telnet logins.

Views

System view

Predefined user roles

network-admin

Parameters

mac: Specifies a Layer 2 ACL. To specify an ACL of a different type, do not specify this keyword.

acl-number: Specifies an ACL by its number. If you specify the **mac** keyword, the value range of this argument is 4000 to 4999. If you do not specify the **mac** keyword, the value range of this argument is 2000 to 3999.

Usage guidelines

This command is not supported in FIPS mode.

You can specify an ACL that does not exist for this command. However, this command takes effect only after you create the ACL and configure rules for the ACL. For more information about ACL, see *ACL and QoS Configuration Guide*.

If you execute this command multiple times, the most recent configuration takes effect.

This command does not take effect on existing Telnet connections.

Examples

Permit only the user at 1.1.1.1 to Telnet to the device.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] telnet server acl 2001
```

telnet server acl-deny-log enable

Use **telnet server acl-deny-log enable** to enable logging for Telnet login attempts that are denied by the Telnet login control ACL.

Use **undo telnet server acl-deny-log enable** to disable logging for Telnet login attempts that are denied by the Telnet login control ACL.

Syntax

telnet server acl-deny-log enable

undo telnet server acl-deny-log enable

Default

Logging is disabled for Telnet login attempts that are denied by the Telnet login control ACL.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Only clients permitted by the Telnet login control ACL can Telnet to the device. This logging feature generates log messages for Telnet login attempts that are denied by the Telnet login control ACL.

For information about log message output, see the information center in *Network Management and Monitoring Configuration Guide*. For information about configuring a Telnet login control ACL, see the **telnet server acl** or **telnet server ipv6 acl** command.

Examples

Enable logging for Telnet login attempts that are denied by the Telnet login control ACL.

```
<Sysname> system-view
[Sysname] telnet server acl-deny-log enable
```

Related commands

telnet server acl

telnet server ipv6 acl

telnet server dscp

Use **telnet server dscp** to specify the DSCP value for IPv4 to use for Telnet packets sent to a Telnet client.

Use **undo telnet server dscp** to restore the default.

Syntax

telnet server dscp *dscp-value*

undo telnet server dscp

Default

IPv4 uses the DSCP value 48 for Telnet packets sent to a Telnet client.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63.

Usage guidelines

This command is not supported in FIPS mode.

The DSCP value is carried in the ToS field of an IPv4 packet to indicate the packet transmission priority.

Examples

Set the DSCP value for IPv4 to use for outgoing Telnet packets to 30 on a Telnet server.

```
<Sysname> system-view
[Sysname] telnet server dscp 30
```

telnet server enable

Use **telnet server enable** to enable the Telnet server.

Use **undo telnet server enable** to disable the Telnet server.

Syntax

telnet server enable

undo telnet server enable

Default

The Telnet server is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command is not supported in FIPS mode.

Users can Telnet to the device only when the Telnet server is enabled.

Examples

Enable the Telnet server.

```
<Sysname> system-view
[Sysname] telnet server enable
```

telnet server ipv6 acl

Use **telnet server ipv6 acl** to apply an IPv6 ACL to filter IPv6 Telnet logins.

Use **undo telnet server ipv6 acl** to restore the default.

Syntax

telnet server ipv6 acl { **ipv6** | **mac** } *acl-number*

undo telnet server ipv6 acl

Default

No IPv6 ACL is used to filter IPv6 Telnet logins.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6: Specifies an IPv6 ACL.

mac: Specifies a Layer 2 ACL. To specify an ACL of a different type, do not specify this keyword.

acl-number: Specifies an ACL by its number. If you specify the **ipv6** keyword, the value range of this argument is 2000 to 3999. If you specify the **mac** keyword, the value range of this argument is 4000 to 4999.

Usage guidelines

This command is not supported in FIPS mode.

You can specify an ACL that does not exist for this command. However, this command takes effect only after you create the ACL and configure rules for the ACL. For more information about ACL, see *ACL and QoS Configuration Guide*.

If you execute this command multiple times, the most recent configuration takes effect.

This command does not take effect on existing Telnet connections.

Examples

Permit only the user at 2000::1 to Telnet to the device.

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2001
[Sysname-acl6-ipv6-basic-2001] rule permit source 2000::1 128
[Sysname-acl6-ipv6-basic-2001] quit
[Sysname] telnet server ipv6 acl ipv6 2001
```

telnet server ipv6 dscp

Use **telnet server ipv6 dscp** to specify the DSCP value for IPv6 to use for Telnet packets sent to a Telnet client.

Use **undo telnet server ipv6 dscp** to restore the default.

Syntax

telnet server ipv6 dscp *dscp-value*

undo telnet server ipv6 dscp

Default

IPv6 uses the DSCP value 48 for Telnet packets sent to a Telnet client.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63.

Usage guidelines

This command is not supported in FIPS mode.

The DSCP value is carried in the Traffic class field of an IPv6 packet to indicate the packet transmission priority.

Examples

Set the DSCP value for IPv6 to use for outgoing Telnet packets to 30 on a Telnet server.

```
<Sysname> system-view
[Sysname] telnet server ipv6 dscp 30
```

telnet server ipv6 port

Use **telnet server ipv6 port** to specify the IPv6 Telnet service port number.

Use **undo telnet server ipv6 port** to restore the default.

Syntax

telnet server ipv6 port *port-number*

undo telnet server ipv6 port

Default

The IPv6 Telnet service port number is 23.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies a port number. The value can be 23 or in the range of 1025 to 65535.

Usage guidelines

This command terminates all existing Telnet connections to the IPv6 Telnet server. To use the Telnet service, users must reestablish Telnet connections.

Examples

Set the IPv6 Telnet service port number to 1026.

```
<Sysname> system-view
[Sysname] telnet server ipv6 port 1026
```

telnet server port

Use **telnet server port** to specify the IPv4 Telnet service port number.

Use **undo telnet server port** to restore the default.

Syntax

telnet server port *port-number*

undo telnet server port

Default

The IPv4 Telnet service port number is 23.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies a port number. The value can be 23 or in the range of 1025 to 65535.

Usage guidelines

This command terminates all existing Telnet connections to the IPv4 Telnet server. To use the Telnet service, users must reestablish Telnet connections.

Examples

Set the IPv4 Telnet service port number to 1025.

```
<Sysname> system-view
[Sysname] telnet server port 1025
```

terminal type

Use **terminal type** to specify the terminal display type.

Use **undo terminal type** to restore the default.

Syntax

terminal type { **ansi** | **vt100** }

undo terminal type

Default

The terminal display type is ANSI.

Views

User line view

User line class view

Predefined user roles

network-admin

Parameters

ansi: Specifies the ANSI type.

vt100: Specifies the VT100 type.

Usage guidelines

The device supports two terminal display types: ANSI and VT100. As a best practice, specify the VT100 type on both the device and the configuration terminal. If either side uses the ANSI type, a display problem might occur when a command line has more than 80 characters. For example, a cursor positioning error might occur.

This command is available in both user line view and user line class view. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.

A terminal display type change does not take effect for the current session. It takes effect for subsequent login sessions.

Examples

Set the terminal display type to VT100.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] terminal type vt100
```

user-interface

Use **user-interface** to enter one or multiple user line views.

Syntax

user-interface { *first-number1* [*last-number1*] | { **aux** | **usb** | **vty** } *first-number2* [*last-number2*] }

Views

System view

Predefined user roles

network-admin

Parameters

first-number1: Specifies the absolute number of the first user line. The value range is 0 to 83.

last-number1: Specifies the absolute number of the last user line. The value range is 1 to 83. This number must be greater than *first-number1*.

aux: Specifies the AUX line.

usb: Specifies the USB line.

vty: Specifies the VTY line.

first-number2: Specifies the relative number of the first user line. The value range is 0 to 9 for AUX and USB lines and 0 to 63 for VTY lines.

last-number2: Specifies the relative number of the last user line. The value range is 1 to 9 for AUX and USB lines and 1 to 63 for VTY lines. This number must be greater than *first-number2*.

Usage guidelines

This command is an older version reserved for backward compatibility purposes. It has the same functionality and output as the **line** command. As a best practice, use the **line** command.

To configure settings for a single user line, use this command to enter the user line view.

To configure the same settings for multiple user lines, use this command to enter multiple user line views.

Examples

Enter the view of AUX line 0.

```
<Sysname> system-view
[Sysname] user-interface aux 0
[Sysname-line-aux0]
```

Enter the views of VTY lines 0 to 4.

```
<Sysname> system-view
[Sysname] user-interface vty 0 4
[Sysname-line-vty0-4]
```

Related commands

user-interface class

user-interface class

Use **user-interface class** to enter user line class view.

Syntax

user-interface class { **aux** | **usb** | **vty** }

Views

System view

Predefined user roles

network-admin

Parameters

aux: Specifies the AUX line class view.

usb: Specifies the USB line.

vty: Specifies the VTY line class view.

Usage guidelines

This command is an older version reserved for backward compatibility purposes. It has the same functionality and output as the **line class** command. As a best practice, use the **line class** command.

To configure the same settings for all user lines of a line class, you can use this command to enter the user line class view.

The following commands are available in user line class view:

- **activation-key**
- **auto-execute command**
- **authentication-mode**
- **command accounting**
- **command authorization**
- **escape-key**
- **history-command max-size**
- **idle-timeout**
- **protocol inbound**
- **screen-length**
- **set authentication password**
- **shell**
- **terminal type**
- **user-role**

For commands that are available in both user line view and user line class view, the device uses the following rules to determine the settings to use:

- A setting in user line view applies only to the user line. A setting in user line class view applies to all user lines of the class.
- A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.
- A setting in user line class view does not take effect for current online users. It takes effect only for new login users.

Examples

Set the CLI connection idle-timeout timer to 15 minutes in VTY line class view.

```
<Sysname> system-view
[Sysname] user-interface class vty
[Sysname-line-class-vty] idle-timeout 15
```

In AUX line class view, configure character **s** as the terminal session activation key.

```
<Sysname> system-view
[Sysname] user-interface class aux
[Sysname-line-class-aux] activation-key s
[Sysname-line-class-aux] quit
```

In the view of AUX line 0, restore the default terminal session activation key.

```
[Sysname] user-interface aux 0
[Sysname-line-aux0] undo activation-key
```

Alternatively, you can use the following command:

```
[Sysname-line-aux0] activation-key 13
```

To verify the configuration:

1. Exit the session on AUX line 0.

   ```
   [Sysname-line-aux0] return
   <Sysname> quit
   ```

2. Log in again through the AUX line.

   The following message appears:

```
Press ENTER to get started.
```

3. Press **Enter**.

   Pressing **Enter** does not start a session.

4. Enter **s**.

   A terminal session is started.

   ```
   <Sysname>
   ```

Related commands

user-interface

user-role

Use **user-role** to assign a user role to a user line. The device assigns the user role to a user of the line when the user logs in.

Use **undo user-role** to remove a user role or restore the default.

Syntax

user-role *role-name*

undo user-role [*role-name*]

Default

A console or USB user is assigned the network-admin user role. Other users are assigned the network-operator user role.

Views

User line view

User line class view

Predefined user roles

network-admin

Parameters

role-name: Specifies a user role name, a case-sensitive string of 1 to 63 characters. The user role can be user-defined or predefined. Available predefined user roles include network-admin, network-operator, and level-0 to level-15. The predefined security-audit and guest-manager user roles are not supported in user line view or user line class view. If you do not specify this argument, the **undo user-role** command restores the default user role.

Usage guidelines

This command is not supported in FIPS mode.

Only users assigned the network-admin, or level-15 user role can execute this command. Other users cannot execute this command, even if they are granted the right to execute this command.

This command is available in both user line view and user line class view. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.

A user role change does not take effect for the current session. It takes effect for subsequent login sessions.

You can assign up to 64 user roles to a user line.

For more information about user roles, see RBAC configuration in *Fundamentals Configuration Guide*.

Examples

Assign user role network-admin to AUX line 0.

```
<Sysname> system-view
[Sysname] line aux 0
[Sysname-line-aux0] user-role network-admin
```

web captcha

Use **web captcha** to specify a fixed verification code for Web login.

Use **undo web captcha** to restore the default.

Syntax

web captcha *verification-code*

undo web captcha

Default

No fixed verification code is specified for Web login. A Web user must enter the verification code displayed on the login page.

Views

User view

Predefined user roles

network-admin

Parameters

verification-code: Specifies the fixed verification code, a case-sensitive 4-character string.

Usage guidelines

In test environments where a script is used for Web function tests, you can configure a fixed verification code to improve test efficiency.

For Web access security purposes, do not use this feature in production environments.

If you execute the **web captcha** command multiple times, the most recent configuration takes effect.

This command is not saved to the configuration file and will not take effect after a reboot.

Examples

Set the fixed verification code to **test** for Web login.

```
<Sysname> web captcha test
```

web https-authorization mode

Use **web https-authorization mode** to set the authentication mode for HTTPS login.

Use **undo web https-authorization mode** to restore the default.

Syntax

web https-authorization mode { **auto** | **manual** }

undo web https-authorization mode

Default

Manual authentication mode is used for HTTPS login.

Views

System view

Predefined user roles

network-admin

Parameters

auto: Uses the PKI certificate of an HTTPS client to authenticate the client automatically.

manual: Sends the login page to the HTTPS client, and uses the username and password entered on the page to authenticate the client.

Usage guidelines

In auto authentication mode, the device uses the PKI certificate of an HTTPS client to authenticate the client automatically.

- If the certificate is valid, the value of the CN field is used as the username for AAA authentication.
  - If the authentication succeeds, the Web interface appears on the client.
  - If the authentication fails, the login page appears on the client. The user can log in to the Web interface after entering the correct username and password.
- If the certificate is invalid (for example, expired), the device closes the HTTPS connection.

Examples

Set the HTTPS login authentication mode to **auto**.

```
<Sysname> system-view
[Sysname] web https-authorization mode auto
```

web idle-timeout

Use **web idle-timeout** to set the Web connection idle-timeout timer.

Use **undo web idle-timeout** to restore the default.

Syntax

web idle-timeout *idle-time*

undo web idle-timeout

Default

The Web connection idle-timeout timer is 10 minutes.

Views

System view

Predefined user roles

network-admin

Parameters

idle-time: Specifies the Web connection idle-timeout timer in minutes. The value range is 1 to 999.

Usage guidelines

The system automatically terminates a Web user connection if no mouse or keyboard operation occurs within the idle-timeout interval.

This command takes effect immediately for current Web connections.

Examples

Set the Web connection idle-timeout timer to 100 minutes.

```
<Sysname> system-view
[Sysname] web idle-timeout 100
```

webui log enable

Use **webui log enable** to enable Web operation logging.

Use **undo webui log enable** to disable Web operation logging.

Syntax

webui log enable

undo webui log enable

Default

Web operation logging is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

When Web operation logging is enabled, the device generates log messages for important Web operations, for example, system time change. The device outputs log messages as indicated by information center settings.

Web operations that can trigger Web operation logging depend on the device model.

A Web operation log message includes the following information:

- Module name **WEB**.
- Mnemonic prefix **WEBOPT**_.
- Web client IP address.
- Web user's username.

The following is a sample log message:

```
%Mar 25 14:32:38:802 2013 H3C WEB/6/WEBOPT_SET_TIME: -HostIP=192.168.100.235-User=Admin;
Set the system date and time to 2013-05-27T10:00:00.
```

Examples

Enable Web operation logging.

```
<Sysname> system-view
[Sysname] webui log enable
```

Contents

FTP commands

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

FTP is not supported in FIPS mode.

FTP server commands

display ftp-server

Use **display ftp-server** to display FTP server configuration and status information.

Syntax

display ftp-server

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display FTP server configuration and status information.

```
<Sysname> display ftp-server
FTP server is running.
User count:                         1
Idle-timeout timer (in minutes):  30
```

Table 1 Command output

Field	Description
User count	Number of the current logged-in users.
Idle-timeout timer (in minutes)	If no packet is exchanged between the FTP server and client during this period, the FTP connection is closed.

Related commands

ftp server enable

ftp timeout

display ftp-user

Use **display ftp-user** to display detailed information about online FTP users.

Syntax

display ftp-user

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display detailed information about online FTP users.

```
<Sysname> display ftp-user
UserName     HostIP             Port     HomeDir
root         192.168.20.184     46539    flash:
```

A field value is wrapped if its length exceeds the limit. The segments are left justified.

The following are the length limits for fields:

- **UserName**—10 characters.
- **HostIP**—15 characters.
- **HomeDir**—37 characters.

```
<Sysname> display ftp-user
UserName     HostIP             Port     HomeDir
user2        2000:2000:2000:    1499     flash:/user2
             2000:2000:2000:
             2000:2000
administra   100.100.100.100    10001    flash:/123456789/123456789/123456789/
tor                                      123456789/123456789/123456789/1234567
                                         89/123456789
```

Table 2 Command output

Field	Description
UserName	Name of the user.
HostIP	IP address of the user.
Port	Port number of the user.
HomeDir	Authorized directory for the user.

free ftp user

Use **free ftp user** to manually release the FTP connections established by using a specific user account.

Syntax

free ftp user *username*

Views

User view

Predefined user roles

network-admin

Parameters

username: Specifies a username. To display online FTP users, execute the **display ftp-user** command.

Examples

Release the FTP connections established by using user account **ftpuser**.

```
<Sysname> free ftp user ftpuser
Are you sure to free FTP connection? [Y/N]:y
<Sysname>
```

free ftp user-ip

Use **free ftp user-ip** to manually release the FTP connections established from a specific IPv4 address.

Syntax

free ftp user-ip *ip-address* [**port** *port*]

Views

User view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the source IP address of an FTP connection. To view the source IP addresses of FTP connections, execute the **display ftp-user** command.

port *port*: Specifies the source port of an FTP connection. To view the source ports of FTP connections, execute the **display ftp-user** command.

Examples

Release the FTP connections established from the IP address 192.168.20.184.

```
<Sysname> free ftp user-ip 192.168.20.184
Are you sure to free FTP connection? [Y/N]:y
<Sysname>
```

free ftp user-ip ipv6

Use **free ftp user-ip ipv6 to** manually release the FTP connections established from a specific IPv6 address.

Syntax

free ftp user-ip ipv6 *ipv6-address* [**port** *port*]

Views

User view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the source IPv6 address of an FTP connection. To view the source IPv6 addresses of FTP connections, execute the **display ftp-user** command.

port *port*: Specifies the source port of an FTP connection. To view the source ports of FTP connections, execute the **display ftp-user** command.

Examples

Release the FTP connections established from IPv6 address 2000::154.

```
<Sysname> free ftp user-ip ipv6 2000::154
Are you sure to free FTP connection? [Y/N]:y
<Sysname>
```

ftp server acl

Use **ftp server acl** to use an ACL to control FTP clients' access to the FTP server.

Use **undo ftp server acl** to restore the default.

Syntax

ftp server acl { *advanced-acl-number* | *basic-acl-number* | **ipv6** { *advanced-acl-number* | *basic-acl-number* } }

undo ftp server acl [**ipv6**]

Default

No ACL is used to control FTP clients' access to the FTP server.

Views

System view

Predefined user roles

network-admin

Parameters

advanced-acl-number: Specifies an advanced IPv4 ACL number in the range of 3000 to 3999.

basic-acl-number: Specifies a basic IPv4 ACL number in the range of 2000 to 2999.

ipv6 *advanced-acl-number*: Specifies an advanced IPv6 ACL number in the range of 3000 to 3999.

ipv6 *basic-acl-number*: Specifies a basic IPv6 ACL number in the range of 2000 to 2999.

Usage guidelines

You can use this command to permit only FTP requests from specific FTP clients. This configuration takes effect only for FTP connections to be established. It does not impact existing FTP connections.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Use ACL 2001 to allow only client 1.1.1.1 to access the FTP server.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule 0 permit source 1.1.1.1 0
[Sysname-acl-ipv4-basic-2001] rule 1 deny source any
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] ftp server acl 2001
```

ftp server acl-deny-log enable

Use **ftp server acl-deny-log enable** to enable logging for FTP login attempts that are denied by the FTP login control ACL.

Use **undo ftp server acl-deny-log enable** to disable logging for FTP login attempts that are denied by the FTP login control ACL.

Syntax

ftp server acl-deny-log enable

undo ftp server acl-deny-log enable

Default

Logging is disabled for FTP login attempts that are denied by the FTP login control ACL.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Only clients permitted by the FTP login control ACL can use FTP to access the device. This logging feature generates log messages for FTP login attempts that are denied by the FTP login control ACL.

For information about log message output, see the information center in *Network Management and Monitoring Configuration Guide*. For information about configuring an FTP login control ACL, see the **ftp server acl** command.

Examples

Enable logging for FTP login attempts that are denied by the FTP login control ACL.

```
<Sysname> system-view
[Sysname] FTP server acl-deny-log enable
```

Related commands

ftp server acl

ftp server dscp

Use **ftp server dscp** to set the DSCP value for IPv4 to use for FTP packets sent to an FTP client.

Use **undo ftp server dscp** to restore the default.

Syntax

ftp server dscp *dscp-value*

undo ftp server dscp

Default

IPv4 uses the DSCP value 0 for FTP packets sent to an FTP client.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63.

Usage guidelines

The DSCP value is carried in the ToS field of an IP packet to indicate the transmission priority of the packet.

Examples

Set the DSCP value for IPv4 to use for outgoing FTP packets to 30 on an FTP server.

```
<Sysname> system-view
[Sysname] ftp server dscp 30
```

ftp server enable

Use **ftp server enable** to enable the FTP server.

Use **undo ftp server enable** to disable the FTP server.

Syntax

ftp server enable

undo ftp server enable

Default

The FTP server is disabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable the FTP server.

```
<Sysname> system-view
[Sysname] ftp server enable
```

ftp server ipv6 dscp

Use **ftp server ipv6 dscp** to set the DSCP value for IPv6 to use for FTP packets sent to an FTP client.

Use **undo ftp server ipv6 dscp** to restore the default.

Syntax

ftp server ipv6 dscp *dscp-value*

undo ftp server ipv6 dscp

Default

IPv6 uses the DSCP value 0 for FTP packets sent to an FTP client.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63.

Usage guidelines

The DSCP value is carried in the Traffic class field of an IPv6 packet to indicate the transmission priority of the packet.

Examples

Set the DSCP value for IPv6 to use for outgoing FTP packets to 30 on an FTP server.

```
<Sysname> system-view
[Sysname] ftp server ipv6 dscp 30
```

ftp server ssl-server-policy

Use **ftp server ssl-server-policy** to associate an SSL server policy with the FTP server.

Use **undo ftp server ssl-server-policy** to restore the default.

Syntax

ftp server ssl-server-policy *policy-name*

undo ftp server ssl-server-policy

Default

No SSL server policy is associated with the FTP server.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies an SSL server policy by its name, a string of 1 to 31 characters.

Usage guidelines

After you associate an SSL server policy with the device, a client that supports SFTP will establish a secure connection to the device to ensure data security.

Examples

Associate SSL server policy **myssl** with the FTP server.

```
<Sysname> system-view
[Sysname] ftp server ssl-server-policy myssl
```

Related commands

ftp server enable

ssl server-policy (*Security Command Reference*)

ftp timeout

Use **ftp timeout** to set the FTP connection idle-timeout timer.

Use **undo ftp timeout** to restore the default.

Syntax

ftp timeout *minute*

undo ftp timeout

Default

The FTP connection idle-timeout timer is 30 minutes.

Views

System view

Predefined user roles

network-admin

Parameters

minute: Specifies a time interval in the range of 1 to 35791 minutes.

Usage guidelines

If no data transfer occurs on an FTP connection within the idle-timeout interval, the FTP server closes the FTP connection to release resources.

Examples

Set the FTP connection idle-timeout timer to 36 minutes.

```
<Sysname> system-view
[Sysname] ftp timeout 36
```

FTP client commands

For FTP users to execute FTP client configuration commands, you must configure authorization settings for users on the FTP server. Authorized operations include viewing the files in the working directory, reading/downloading/uploading/renaming/removing files, and creating directories.

The FTP client commands in this section are supported by the device, but whether they can be executed successfully depends on the FTP server.

The output in the examples of this section varies by FTP server type.

?

Use **?** to display all commands supported by an FTP client.

Use **?** *command-name* to display the help information for a command.

Syntax

? [*command-name*]

Views

FTP client view

Predefined user roles

network-admin

Parameters

command-name: Specifies a command supported by the FTP client.

Usage guidelines

In FTP client view, entering **?** is the same as executing the **help** command.

Examples

Display all commands supported by the FTP client.

```
ftp> ?
Commands may be abbreviated.  Commands are:

append          delete          ls              quit            rmdir
ascii           debug           mkdir           reget           status
binary          dir             newer           rstatus         system
bye             disconnect      open            rhelp           user
cd              get             passive         rename          verbose
cdup            help            put             reset           ?
close           lcd             pwd             restart
```

Display the help information for the **dir** command.

```
ftp> ? dir
dir              list contents of remote directory
```

Related commands

help

append

Use **append** to add the content of a file on the FTP client to a file on the FTP server.

Syntax

append *localfile* [*remotefile*]

Views

FTP client view

Predefined user roles

network-admin

Parameters

localfile: Specifies a file on the FTP client.

remotefile: Specifies a file on the FTP server.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

Examples

Append the content of the local **a.txt** file to the **b.txt** file on the FTP server.

```
ftp> append a.txt b.txt
227 Entering Passive Mode (192,168,1,84,8,145)
150 Accepted data connection
226 File successfully transferred
1657 bytes sent in 0.000736 seconds (2.15 Mbyte/s)
```

ascii

Use **ascii** to set the file transfer mode to ASCII.

Syntax

ascii

Default

The file transfer mode is binary.

Views

FTP client view

Predefined user roles

network-admin

Usage guidelines

You can perform this operation only after you log in to the FTP server.

FTP transfers files in either of the following modes:

- **Binary mode**—Transfers non-text files.
- **ASCII mode**—Transfers text files.

When the device acts as the FTP server, the transfer mode is determined by the FTP client. When the device acts as the FTP client, you can set the transfer mode. The transfer mode is binary by default.

Examples

Set the file transfer mode to ASCII.

```
ftp> ascii
200 TYPE is now ASCII
```

Related commands

binary

binary

Use **binary** to set the file transfer mode to binary, which is also called the flow mode.

Syntax

binary

Default

The file transfer mode is binary.

Views

FTP client view

Predefined user roles

network-admin

Usage guidelines

You can perform this operation only after you log in to the FTP server.

FTP transfers files in either of the following modes:

- **Binary mode**—Transfers program file or pictures.

- **ASCII mode**—Transfers text files.

When the device acts as the FTP server, the transfer mode is determined by the FTP client. When the device acts as the FTP client, you can set the transfer mode. The default transfer mode is binary.

Examples

Set the file transfer mode to binary.

```
ftp> binary
200 TYPE is now 8-bit binary
```

Related commands

ascii

bye

Use **bye** to terminate the connection to the FTP server and return to user view. If no connection is established between the device and the FTP server, use this command to return to user view.

Syntax

bye

Views

FTP client view

Predefined user roles

network-admin

Examples

Terminate the connection to the FTP server and return to user view.

```
ftp> bye
221-Goodbye. You uploaded 2 and downloaded 2 kbytes.
221 Logout.
<Sysname>
```

Related commands

quit

cd

Use **cd** to change the current working directory to another directory on the FTP server.

Syntax

cd { *directory* | **..** | **/** }

Views

FTP client view

Predefined user roles

network-admin

Parameters

directory: Specifies the target directory. If the target directory does not exist, the **cd** command does not change the current working directory.

..: Specifies the upper directory. Executing the **cd ..** command is the same as executing the **cdup** command. If the current working directory is the FTP root directory, the **cd ..** command does not change the current working directory.

/: Specifies the FTP root directory.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

The directory that can be accessed must be authorized by the FTP server.

Examples

Change the working directory to the **logfile** subdirectory of the current directory.

```
ftp> cd logfile
250 OK. Current directory is /logfile
```

Change the working directory to the **folder** subdirectory of the FTP root directory.

```
ftp> cd /folder
250 OK. Current directory is /folder
```

Change the working directory to the upper directory of the current directory.

```
ftp> cd ..
250 OK. Current directory is /
```

Change the working directory to the FTP root directory.

```
ftp> cd /
250 OK. Current directory is /
```

Related commands

cdup

pwd

cdup

Use **cdup** to enter the upper directory of the FTP server.

Syntax

cdup

Views

FTP client view

Predefined user roles

network-admin

Usage guidelines

You can perform this operation only after you log in to the FTP server.

This command does not change the working directory if the current directory is the FTP root directory.

Examples

Change the working directory to the upper directory.

```
ftp> pwd
257 "/ftp/subdir" is your current location
ftp> cdup
250 OK. Current directory is /ftp
```

```
ftp> pwd
257 "/ftp" is your current location
```

Related commands

cd

pwd

close

Use **close** to terminate the connection to the FTP server without exiting FTP client view.

Syntax

close

Views

FTP client view

Predefined user roles

network-admin

Usage guidelines

You can perform this operation only after you log in to the FTP server.

Examples

Terminate the connection to the FTP server without exiting the FTP client view.

```
ftp> close
221-Goodbye. You uploaded 0 and downloaded 0 kbytes.
221 Logout.
ftp>
```

Related commands

disconnect

debug

Use **debug** to enable or disable FTP client debugging.

Syntax

debug

Default

FTP client debugging is disabled.

Views

FTP client view

Predefined user roles

network-admin

Usage guidelines

When FTP client debugging is enabled, executing this command disables FTP client debugging.

When FTP client debugging is disabled, executing this command enables FTP client debugging.

Examples

Enable and then disable FTP client debugging.

```
ftp> debug
Debugging on (debug=1).
ftp> debug
Debugging off (debug=0).
```

delete

Use **delete** to permanently delete a file from the FTP server.

Syntax

delete *remotefile*

Views

FTP client view

Predefined user roles

network-admin

Parameters

remotefile: Specifies a file on the FTP server.

Usage guidelines

CAUTION:

Permanently delete a file from the FTP server with caution. When you permanently delete a file from the FTP server, make sure the file is no longer in use.

You can perform this operation only after you log in to the FTP server.

To perform this operation, you must have delete permission on the FTP server.

Examples

Delete the **b.txt** file.

```
ftp> delete b.txt
250 Deleted b.txt
```

dir

Use **dir** to display or save detailed information about files and directories on the FTP server.

Syntax

dir [*remotefile* [*localfile*]]

Views

FTP client view

Predefined user roles

network-admin

Parameters

remotefile: Specifies a file or directory on the FTP server.

localfile: Specifies the name of the local file used to save the displayed information.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

To display detailed information about the files and subdirectories in the working directory on the FTP server, use the **dir** command.

To display detailed information about a file or directory on the FTP server, use the **dir** *remotefile* command.

To save detailed information about a file or directory on the FTP server to a local file, use the **dir** *remotefile localfile* command.

In FTP client view, executing the **dir** command is the same as executing the **ls** command.

Examples

Display detailed information about the files and subdirectories in the working directory on the FTP server.

```
ftp> dir
150 Connecting to port 50201
-rwxr-xr-x    1 0          0                1481 Jul  7 15:36 a.txt
drwxr-xr-x    2 0          0                8192 Jul  2 14:33 diagfile
drwxr-xr-x    3 0          0                8192 Jul  7 15:21 ftp
drwxr-xr-x    2 0          0                8192 Jul  5 09:15 logfile
drwxr-xr-x    2 0          0                8192 Jul  2 14:33 seclog
-rwxr-xr-x    1 0          0            40808448 Jul  2 14:33 system-a1801.bin
-rwxr-xr-x    1 0          0                3050 Jul  7 12:26 startup.cfg
-rwxr-xr-x    1 0          0               54674 Jul  4 09:24 startup.mdb
-rwxr-xr-x    1 0          0                1481 Jul  7 12:34 x.cfg
226 9 matches total
```

Save detailed information about file **a.txt** to **s.txt**.

```
ftp> dir a.txt s.txt
output to local-file: s.txt ? [Y/N]y
150 Connecting to port 50203
226-Glob: a.txt
```

Display the content of the file **s.txt**.

```
ftp> bye
221-Goodbye. You uploaded 0 and downloaded 2 kbytes.
221 Logout.
<Sysname> more s.txt
-rwxr-xr-x    1 0          0                1481 Jul  7 12:34 a.txt
```

Related commands

ls

disconnect

Use **disconnect** to terminate the connection to the FTP server without exiting FTP client view.

Syntax

disconnect

Views

FTP client view

Predefined user roles

network-admin

Usage guidelines

You can perform this operation only after you log in to the FTP server.

Examples

Terminate the connection to the FTP server without exiting the FTP client view.

```
ftp> disconnect
221-Goodbye. You uploaded 0 and downloaded 0 kbytes.
221 Logout.
ftp>
```

Related commands

close

display ftp client source

Use **display ftp client source** to display the source address settings on the FTP client.

Syntax

display ftp client source

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the source address settings on the FTP client.

```
<Sysname> display ftp client source
The source IP address of the FTP client is 1.1.1.1.
```

ftp

Use **ftp** to log in to an IPv4 FTP server and enter FTP client view.

Syntax

ftp [*ftp-server* [*service-port*] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* } | **-d**] *]

Views

User view

Predefined user roles

network-admin

Parameters

ftp-server: Specifies the IPv4 address or host name of an FTP server. A host name can be a case-insensitive string of 1 to 253 characters. Valid characters for a host name include letters, digits, hyphens (-), underscores (_), and dots (.).

service-port: Specifies the TCP port number of the FTP server, in the range of 0 to 65535. The default is 21.

dscp *dscp-value*: Specifies the DSCP value for IPv4 to use in outgoing FTP packets to indicate the packet transmission priority. The value range is 0 to 63. The default is 0.

source { **interface** *interface-type interface-number* | **ip** *source-ip-address* }: Specifies the source address used to establish the FTP connection.

- **interface** *interface-type interface-number*: Specifies an interface by its type and number. The device will use the interface's primary IPv4 address as the source address. To establish the FTP connection successfully, make sure the interface is up and has the primary IPv4 address configured.
- **ip** *source-ip-address*: Specifies an IPv4 address. To establish the FTP connection successfully, make sure this address is the IPv4 address of an interface in up state on the device.

-d: Enables FTP client debugging.

Usage guidelines

This command is only applicable to IPv4 networks.

If no parameters are specified, this command enters the FTP client view without logging in to an FTP server.

If the server parameters are specified, you are prompted to enter the username and password for logging in to the FTP server.

Examples

Log in to FTP server 192.168.0.211. Use 192.168.0.212 as the source IPv4 address for outgoing FTP packets.

```
<Sysname>ftp 192.168.0.211 source ip 192.168.0.212
Press CTRL+C to abort.
Connected to 192.168.0.211 (192.168.0.211).
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User (192.168.0.211:(none)): abc
331 Give me your password, please
Password:
230 Logged in successfully
Remote system type is MSDOS.
ftp>
```

Log in to FTP server 192.168.0.211 and enable FTP client debugging.

```
<Sysname> ftp 192.168.0.211 –d
Press CTRL+C to abort.
Connected to 192.168.0.211 (192.168.0.211).
220 FTP service ready.
User (192.168.0.211:(none)): abc
*Apr 10 09:02:24:139 2017 Sysname FTPC/7/EVENT: PAM initialization result: 0.
*Apr 10 09:02:24:150 2017 Sysname FTPC/7/EVENT: PAM: Sent a start-accounting request.
Result: 0.
*Apr 10 09:02:24:860 2017 Sysname FTPC/7/COMMAND: USER abc
331 Password required for abc.
Password:
*Apr 10 09:02:25:575 2017 Sysname FTPC/7/COMMAND: PASS XXXX
230 User logged in.
```

```
215 UNIX Type: L8
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> *Apr 10 09:02:25:640 2017 SIMWARE FTPC/7/COMMAND: SYST
ftp>
```

ftp client ipv6 source

Use **ftp client ipv6 source** to specify the source IPv6 address for FTP packets sent to an IPv6 FTP server.

Use **undo ftp client ipv6 source** to restore the default.

Syntax

ftp client ipv6 source { **interface** *interface-type interface-number* | **ipv6** *source-ipv6-address* }

undo ftp client ipv6 source

Default

No source address is specified for FTP packets sent to an IPv6 FTP server. The device selects a source IPv6 address as defined in RFC 3484.

Views

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. The device will use the interface's IPv6 address as the source address. For successful FTP packet transmission, make sure the interface is up and is configured with an IPv6 address.

ipv6 *source-ipv6-address*: Specifies an IPv6 address. For successful FTP packet transmission, make sure this address is the IPv6 address of an interface in up state on the device.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

The source address specified with the **ftp ipv6** command takes precedence over the source address specified with the **ftp client ipv6 source** command.

The source address specified with the **ftp client ipv6 source** command applies to all FTP connections. The source address specified with the **ftp ipv6** command applies only to the FTP connection that is being established.

Examples

Specify the source IPv6 address of 2000::1 for FTP packets sent to an IPv6 FTP server.

```
<Sysname> system–view
[Sysname] ftp client ipv6 source ipv6 2000::1
```

Related commands

ftp ipv6

ftp client source

Use **ftp client source** to specify the source IPv4 address for FTP packets sent to an IPv4 FTP server.

Use **undo ftp client source** to restore the default.

Syntax

ftp client source { **interface** *interface-type interface-number* | **ip** *source-ip-address* }

undo ftp client source

Default

No source IPv4 address is specified for FTP packets sent to an IPv4 FTP server. The device uses the primary IPv4 address of the output interface for the route to the server as the source address.

Views

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. The device will use the interface's primary IPv4 address as the source address. For successful FTP packet transmission, make sure the interface is up and has the primary IPv4 address configured.

ip *source-ip-address*: Specifies an IPv4 address. For successful FTP packet transmission, make sure this address is the IPv4 address of an interface in up state on the device.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

The source address specified with the **ftp** command takes precedence over the source address specified with the **ftp client source** command.

The source address specified with the **ftp client source** command applies to all FTP connections. The source address specified with the **ftp** command applies only to the FTP connection that is being established.

Examples

Specify the source IPv4 address of 192.168.20.222 for FTP packets sent to an IPv4 FTP server.

```
<Sysname> system-view
[Sysname] ftp client source ip 192.168.20.222
```

Related commands

ftp

ftp ipv6

Use **ftp ipv6** to log in to an IPv6 FTP server and enter FTP client view.

Syntax

ftp ipv6 [*ftp-server* [*service-port*] [**dscp** *dscp-value* | **source** { **ipv6** *source-ipv6-address* | **interface** *interface-type interface-number* } | **-d**] * [**-i** *interface-type interface-number*]]

Views

User view

Predefined user roles

network-admin

Parameters

ftp-server: Specifies the IPv6 address or host name of an FTP server. A host name can be a case-insensitive string of 1 to 253 characters. Valid characters for a host name include letters, digits, hyphens (-), underscores (_), and dots (.).

service-port: Specifies the TCP port number of the FTP server, in the range of 0 to 65535. The default is 21.

dscp *dscp-value*: Specifies the DSCP value for IPv6 to use in outgoing FTP packets to indicate the packet transmission priority. The value range is 0 to 63. The default is 0.

source { **ipv6** *source-ipv6-address* | **interface** *interface-type interface-number* }: Specifies the source address used to establish the FTP connection.

- **interface** *interface-type interface-number*: Specifies an interface by its type and number. This option can be used only when the FTP server address is a link local address and the specified output interface has a link local address. For information about link local addresses, see *Layer 3—IP Services Configuration Guide*.
- **ipv6** *source-ipv6-address*: Specifies an IPv6 address. To establish the FTP connection successfully, make sure this address is the IPv6 address of an interface in up state on the device.

-i *interface-type interface-number*: Specifies an output interface by its type and number. This option can be used only when the FTP server address is a link local address and the specified output interface has a link local address.

-d: Enables FTP client debugging.

Usage guidelines

This command is only applicable to IPv6 networks.

If no parameters are specified, this command enters the FTP client view.

If the FTP server parameters are specified, you are prompted to enter the username and password for logging in to the FTP server.

Examples

Log in to FTP server 2000::154.

```
<Sysname>ftp ipv6 2000::154
Press CTRL+C to abort.
Connected to 2000::154 (2000::154).
220 FTP service ready.
User (2000::154): root
331 Password required for root.
Password:
230 User logged in
Remote system type is H3C
```

Log in to FTP server 2000::154 and enable FTP client debugging.

```
<Sysname> ftp ipv6 2000::154 –d
Press CTRL+C to abort.
Connected to 2000::154 (2000::154).
220 FTP service ready.
User (2000::154:(none)): root
*Apr 10 09:03:24:139 2017 Sysname FTPC/7/EVENT: PAM initialization result: 0.
*Apr 10 09:03:24:150 2017 Sysname FTPC/7/EVENT: PAM: Sent a start-accounting request.
Result: 0.
*Apr 10 09:03:24:860 2017 Sysname FTPC/7/COMMAND: USER root
331 Password required for root.
Password:
*Apr 10 09:03:25:575 2017 Sysname FTPC/7/COMMAND: PASS XXXX
230 User logged in.
215 UNIX Type: L8
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> *Apr 10 09:03:25:640 2017 SIMWARE FTPC/7/COMMAND: SYST
ftp>
```

get

Use **get** to download a file from the FTP server and save the file.

Syntax

get *remotefile* [*localfile*]

Views

FTP client view

Predefined user roles

network-admin

Parameters

remotefile: Specifies the file to be downloaded.

localfile: Specifies a name for the downloaded file. If you do not specify this argument, the system uses the name of the source file.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

To save the downloaded file to the working directory accessed by the **ftp** command, perform one of the following tasks:

- Execute the command without specifying the *localfile* argument.
- Specify a file name without any path information for the *localfile* argument, for example, a.cfg.

To save the downloaded file to some other directory, you must specify a fully qualified file name for the *localfile* argument, for example, flash:/subdirectory/a.cfg.

Examples

Download the **a.txt** file and save it as **b.txt** in the working directory accessed by the **ftp** command.

```
ftp> get a.txt b.txt
local: b.txt remote: a.txt
150 Connecting to port 47457
226 File successfully transferred
1569 bytes received in 0.00527 seconds (290.6 kbyte/s)
```

Download the **a.txt** file to the **test** directory in the working directory accessed by the **ftp** command.

```
ftp> get a.txt flash:/test/b.txt
local: flash:/test/b.txt remote: a.txt
150 Connecting to port 47457
226 File successfully transferred
1569 bytes received in 0.00527 seconds (290.6 kbyte/s)
```

Download the **a.txt** file to the root directory of the flash memory on a member device. Save the file as **c.txt**.

```
ftp> get a.txt slot1#flash:/c.txt
local: slot1#flash:/c.txt remote: a.txt
150 Connecting to port 47460
226 File successfully transferred
1569 bytes received in 0.0564 seconds (27.2 kbyte/s)
```

Related commands

put

help

Use **help** to display all commands supported by the FTP client.

Use **help** *command-name* to display the help information for a command.

Syntax

help [*command-name*]

Views

FTP client view

Predefined user roles

network-admin

Parameters

command-name: Specifies a command supported by the FTP client.

Usage guidelines

In FTP client view, executing the **help** command is the same as entering **?**.

Examples

Display all commands supported by the FTP client.

```
ftp> help

append          delete          ls              quit            rmdir
ascii           debug           mkdir           reget           status
binary          dir             newer           rstatus         system
bye             disconnect      open            rhelp           user
```

```
cd              get             passive         rename          verbose
cdup            help            put             reset           ?
close           lcd             pwd             restart
```

Display the help information for the **dir** command.

```
ftp> help dir
dir              list contents of remote directory
```

Related commands

?

lcd

Use **lcd** to display or change the local working directory of the FTP client.

Syntax

lcd [*directory* | **/**]

Views

FTP client view

Predefined user roles

network-admin

Parameters

directory: Changes the local working directory of the FTP client to the specified local directory. There must be a slash sign (/) before the name of the storage medium, for example, /flash:/logfile.

/: Changes the local working directory of the FTP client to the local root directory.

Usage guidelines

To display the local working directory of the FTP client, do not specify the *directory* or **/** argument.

Examples

Display the local working directory.

```
ftp> lcd
Local directory now /flash:
```

Change the local working directory to **flash:/logfile**.

```
ftp> lcd /flash:/logfile
Local directory now /flash:/logfile
```

ls

Use **ls** to display or save detailed information about files and directories on the FTP server.

Syntax

ls [*remotefile* [*localfile*]]

Views

FTP client view

Predefined user roles

network-admin

Parameters

remotefile: Specifies a file or directory on the FTP server.

localfile: Specifies the name of the local file used to save the displayed information.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

To display detailed information about the files and subdirectories in the working directory on the FTP server, use the **ls** command.

To display detailed information about a file or directory on the FTP server, use the **ls** *remotefile* command.

To save detailed information about a file or directory on the FTP server to a local file, use the **ls** *remotefile localfile* command.

In FTP client view, executing the **ls** command is the same as executing the **dir** command.

Examples

Display detailed information about the files and subdirectories in the working directory on the FTP server.

```
ftp> ls
150 Connecting to port 50201
-rwxr-xr-x    1 0          0               1481 Jul  7 15:36 a.txt
drwxr-xr-x    2 0          0               8192 Jul  2 14:33 diagfile
drwxr-xr-x    3 0          0               8192 Jul  7 15:21 ftp
drwxr-xr-x    2 0          0               8192 Jul  5 09:15 logfile
drwxr-xr-x    2 0          0               8192 Jul  2 14:33 seclog
-rwxr-xr-x    1 0          0           40808448 Jul  2 14:33 system-a1801.bin
-rwxr-xr-x    1 0          0               3050 Jul  7 12:26 startup.cfg
-rwxr-xr-x    1 0          0              54674 Jul  4 09:24 startup.mdb
-rwxr-xr-x    1 0          0               1481 Jul  7 12:34 x.cfg
226 9 matches total
```

Save detailed information about the file **a.txt** to **s.txt**.

```
ftp> ls a.txt s.txt
output to local-file: s.txt ? [Y/N]y
150 Connecting to port 50203
226-Glob: s.txt
```

Display the content of the file **s.txt**.

```
ftp> bye
221-Goodbye. You uploaded 0 and downloaded 2 kbytes.
221 Logout.
<Sysname> more s.txt
-rwxr-xr-x    1 0          0               1481 Jul  7 12:34 a.txt
```

Related commands

dir

mkdir

Use **mkdir** to create a subdirectory in the current directory on the FTP server.

Syntax

mkdir *directory*

Views

FTP client view

Predefined user roles

network-admin

Parameters

directory: Specifies the name for the directory to be created.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

You must have permission to perform this operation on the FTP server.

Examples

Create a subdirectory named **newdir** in the current directory of the FTP server.

```
ftp> mkdir newdir
257 "newdir" : The directory was successfully created
```

newer

Use **newer** to update a local file by using a file on the FTP server.

Syntax

newer *remotefile* [*localfile*]

Views

FTP client view

Predefined user roles

network-admin

Parameters

remotefile: Specifies a file on the FTP server.

localfile: Specifies the local file to be updated.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

If the local file does not exist, this command downloads the file from the FTP server and saves it locally.

If the file on the FTP server is not newer than the local file, this command does not update the local file.

Examples

Update the local file with the **a.txt** file on the FTP server.

```
ftp> newer a.txt
local: a.txt remote: a.txt
150 Connecting to port 63513
226 File successfully transferred
1573 bytes received in 0.0293 seconds (52.3 kbyte/s)
```

open

Use **open** to log in to an FTP server from FTP client view.

Syntax

open *server-address* [*service-port*]

Views

FTP client view

Predefined user roles

network-admin

Parameters

server-address: Specifies the IPv4 address, IPv6 address, or host name of the FTP server.

service-port: Specifies the TCP port number of the FTP server, in the range of 0 to 65535. The default is 21.

Usage guidelines

After you issue this command, the system will prompt you to enter the username and password.

After you log in to one FTP server, you must disconnect from the server before you can use the **open** command to log in to another server.

Examples

In FTP client view, log in to FTP server 192.168.40.7.

```
<Sysname>ftp
ftp> open 192.168.40.7
Press CTRL+C to abort.
Connected to 192.168.40.7 (192.168.40.7).
220 FTP service ready.
User (192.168.40.7:(none)): root
331 Password required for root.
Password:
230 User logged in.
Remote system type is H3C.
ftp>
```

passive

Use **passive** to change the FTP operation mode.

Syntax

passive

Default

The FTP operation mode is passive.

Views

FTP client view

Predefined user roles

network-admin

Usage guidelines

FTP can operate in either of the following modes:

- **Active mode**—The FTP server initiates the TCP connection.
- **Passive mode**—The FTP client initiates the TCP connection.

When the FTP operation mode is passive, executing this command changes the mode to active.

When the FTP operation mode is active, executing this command changes the mode to passive.

This command is typically used together with a firewall to control FTP session establishment between private network users and public network users.

Examples

Change the FTP operation mode to passive.

```
ftp> passive
Passive mode on.
ftp> passive
Passive mode off.
```

put

Use **put** to upload a file from the FTP client to the FTP server.

Syntax

put *localfile* [*remotefile*]

Views

FTP client view

Predefined user roles

network-admin

Parameters

localfile: Specifies the local file to be uploaded.

remotefile: Specifies the name of the file for saving the uploaded file on the FTP server.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

To upload a file in the current working directory, specify a file name without the path for the *localfile* argument, for example, a.cfg.

To upload a file in some other directory, specify a fully qualified file name for the *localfile* argument, for example, flash:/subdirectory/a.cfg.

Examples

Upload the **a.txt** file from the local working directory to the FTP server. Save the file as **b.txt**.

```
ftp> put a.txt b.txt
local: a.txt remote: b.txt
150 Connecting to port 47461
226 File successfully transferred
1569 bytes sent in 0.000671 seconds (2.23 Mbyte/s)
```

Upload the **a.txt** file from the **test** directory of the local working directory to the FTP server. Save the file as **b.txt**.

```
ftp> put flash:/test/a.txt b.txt
```

```
local: flash:/test/a.txt remote: b.txt
150 Connecting to port 47461
226 File successfully transferred
1569 bytes sent in 0.000671 seconds (2.23 Mbyte/s)
```

Upload file **a.txt** from the **test** directory of the storage medium on a member device. Save the file as **b.txt** on the FTP server.

```
ftp> put slot2#flash:/test/a.txt b.txt
local: slot2#flash:/test/a.txt remote: b.txt
150 Connecting to port 47461
226 File successfully transferred
1569 bytes sent in 0.000671 seconds (2.23 Mbyte/s)
```

Related commands

get

pwd

Use **pwd** to display the currently accessed directory on the FTP server.

Syntax

pwd

Views

FTP client view

Predefined user roles

network-admin

Usage guidelines

You can perform this operation only after you log in to the FTP server.

Examples

Display the currently accessed directory on the FTP server.

```
ftp> cd subdir
250 OK. Current directory is /subdir
ftp> pwd
257 "/subdir" is your current location
```

quit

Use **quit** to terminate the connection to the FTP server and return to user view.

Syntax

quit

Views

FTP client view

Predefined user roles

network-admin

Examples

Terminate the connection to the FTP server and return to user view.

```
ftp> quit
221-Goodbye. You uploaded 0 and downloaded 0 kbytes.
221 Logout.
<Sysname>
```

Related commands

bye

reget

Use **reget** to get the missing part of a file from the FTP server.

Syntax

reget *remotefile* [*localfile*]

Views

FTP client view

Predefined user roles

network-admin

network-operator

Parameters

remotefile: Specifies a file on the FTP server.

localfile: Specifies a local file.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

If a file download is not completed due to network or storage space problems, use this command to get the part that has not been downloaded yet.

Examples

Get the part of the **s.bin** file that has not been downloaded yet.

```
ftp> reget s.bin
local: s.bin remote: s.bin
350 Restarting at 1749706
150-Connecting to port 47429
150 38143.3 kbytes to download
226 File successfully transferred
39058742 bytes received in 66.2 seconds (576.1 kbyte/s)
```

rename

Use **rename** to rename a file.

Syntax

rename [*oldfilename* [*newfilename*]]

Views

FTP client view

Predefined user roles

network-admin

Parameters

oldfilename: Specifies the original file name.

newfilename: Specifies the new file name.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

Examples

Rename the **a.txt** file as **b.txt**.

- Method 1:

```
ftp> rename
(from-name) a.txt
(to-name) b.txt
350 RNFR accepted - file exists, ready for destination
250 File successfully renamed or moved
```

- Method 2:

```
ftp> rename a.txt
(to-name) b.txt
350 RNFR accepted - file exists, ready for destination
250 File successfully renamed or moved
```

- Method 3:

```
ftp> rename a.txt b.txt
350 RNFR accepted - file exists, ready for destination
250 File successfully renamed or moved
```

reset

Use **reset** to clear the reply information received from the FTP server in the buffer.

Syntax

reset

Views

FTP client view

Predefined user roles

network-admin

Examples

Clear the reply information received from the FTP server.

```
ftp> reset
```

restart

Use **restart** to specify the file retransmission offset.

Syntax

restart *marker*

Views

FTP client view

Predefined user roles

network-admin

Parameters

marker: Specifies the retransmission offset, in bytes.

Usage guidelines

Use this command to continue with a file retransmission. The file retransmission starts from the (offset+1)th byte.

You can perform this operation only after you log in to the FTP server.

Support for this command depends on the FTP server.

Examples

Set retransmission offset to 2 bytes and retransmit the **h.c** file. The file has 82 bytes in total.

```
ftp> restart 2
restarting at 2. execute get, put or append to initiate transfer
ftp> put h.c h.c
local: h.c remote: h.c
350 Restart position accepted (2).
150 Ok to send data.
226 File receive OK.
80 bytes sent in 0.000445 seconds (175.6 kbyte/s)
ftp> dir
150 Here comes the directory listing.
-rw-r--r--    1 0        0              82 Jul 18 02:58 h.c
```

rhelp

Use **rhelp** to display the FTP commands supported by the FTP server.

Use **rhelp** *protocol-command* to display the help information for an FTP command supported by the FTP server.

Syntax

rhelp [*protocol-command*]

Views

FTP client view

Predefined user roles

network-admin

Parameters

protocol-command: Specifies an FTP command.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

Examples

Display the FTP-related commands supported by the FTP server.

```
ftp> rhelp
214-The following FTP commands are recognized
 USER PASS NOOP QUIT SYST TYPE
 HELP CWD  XCWD PWD  CDUP XCUP
 XPWD LIST NLST MLSD PORT EPRT
 PASV EPSV REST RETR STOR APPE
 DELE MKD  XMKD RMD  XRMD ABOR
 SIZE RNFR RNTO
214 UNIX Type: L8
```

Table 3 Command output

Field	Description
USER	Username.
PASS	Password.
NOOP	Null operation.
SYST	System parameters.
TYPE	Request type.
CWD	Changes the current working directory.
XCWD	Extended command with the meaning of CWD.
PWD	Prints the working directory.
CDUP	Changes the directory to the upper directory.
XCUP	Extended command with the meaning of CDUP.
XPWD	Extended command with the meaning of PWD.
LIST	Lists files.
NLST	Lists brief file description.
MLSD	Lists file content.
PORT	Active mode (IPv4).
EPRT	Active mode (IPv6).
PASV	Passive mode (IPv4).
EPSV	Passive mode (IPv6).
REST	Restarts.
RETR	Downloads files.
STOR	Uploads files.
APPE	Appends uploading.
DELE	Deletes files.
MKD	Creates folders.
XMKD	Extended command with the meaning of MKD.
RMD	Deletes folders.
XRMD	Extended command with the meaning of RMD.
ABOR	Aborts the transmission.

Field	Description
SIZE	Size of the transmission file.
RNFR	Original name.
RNTO	New name.

rmdir

Use **rmdir** to permanently delete a directory from the FTP server.

Syntax

rmdir *directory*

Views

FTP client view

Predefined user roles

network-admin

Parameters

directory: Specifies a directory on the FTP server.

Usage guidelines

CAUTION:

Permanently delete a directory from the FTP server with caution. When you permanently delete a directory from the FTP server, make sure the directory is no longer in use.

You can perform this operation only after you log in to the FTP server.

To perform this operation, you must have delete permission on the FTP server.

Delete all files and subdirectories in a directory before you delete the directory. For more information about how to delete files, see the **delete** command.

The **rmdir** command does not delete the files of the specified directory from the recycle bin.

Examples

Delete empty directory **subdir1**.

```
ftp>rmdir subdir1
250 The directory was successfully removed
```

Related commands

delete

rstatus

Use **rstatus** to display FTP server status information.

Use **rstatus** *remotefile* to display detailed information about a directory or file on the FTP server.

Syntax

rstatus [*remotefile*]

Views

FTP client view

Predefined user roles

network-admin

Parameters

remotefile: Specifies a directory or file on the FTP server.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

Support for this command depends on the FTP server.

Examples

Display FTP server status information.

```
ftp> rstatus
211-FTP server status:
     Connected to 192.168.20.177
     Logged in as root
     TYPE: ASCII
     No session bandwidth limit
     Session timeout in seconds is 300
     Control connection is plain text
     Data connections will be plain text
     At session startup, client count was 1
     vsFTPd 2.0.6 - secure, fast, stable
211 End of status
```

Table 4 Command output

Filed	Description
211-FTP server status:	Beginning of the display of FTP server status, where 211 specifies the FTP command.
Connected to 192.168.20.177	IP address of the FTP client.
Logged in as root	Login username root.
TYPE: ASCII	File transfer mode ASCII.
Session timeout in seconds is 300	FTP connection idle-timeout interval is 300 seconds.
Control connection is plain text	Control connection type is plain text.
Data connections will be plain text	Data connection type is plain text.
At session startup, client count was 1	FTP connection number is 1.
vsFTPd 2.0.6 - secure, fast, stable	FTP version is 2.0.6.
211 End of status	End of the display of FTP server status.

Display the file **a.txt**.

```
ftp> rstatus a.txt
213-Status follows:
-rw-r--r--    1 0        0             80 Jul 18 02:58 a.txt
213 End of status
```

Table 5 Command output

Field	Description
213-Status follows:	Beginning of the display of the file, where 213 specifies the FTP command.
-rw-r--r--	The first bit specifies the file type. • **-**—Common. • **B**—Block. • **c**—Character. • **d**—Directory. • **l**—Symbol connection file. • **p**—Pipe. • **s**—socket. The second bit through the tenth bit are divided into three groups. Each group contains three characters, representing the access permission of the owner, group, and other users. • **-**—No permission. • **r**—Read permission. • **w**—Write permission. • **x**—Execution permission.
1	Number of connections.
0	Name of the file owner.
0	Group number of the file owner.
80	File size, in bytes.
Jul 18 02:58	Date and time when the file was most recently modified.
a.txt	File name.
213 End of status	End of the display of the file information.

status

Use **status** to display FTP status information.

Syntax

status

Views

FTP client view

Predefined user roles

network-admin

Examples

Display FTP status information.

```
ftp> status
Connected to 192.168.1.56.
No proxy connection.
Not using any security mechanism.
Mode: stream; Type: ascii; Form: non-print; Structure: file
Verbose: on; Bell: off; Prompting: on; Globbing: off
Store unique: off; Receive unique: off
```

```
Case: off; CR stripping: on
Ntrans: off
Nmap: off
Hash mark printing: off; Use of PORT cmds: on
```

Table 6 Command output

Field	Description
Connected to 192.168.1.56.	IP address of the FTP server that is connected to the FTP client.
Verbose: on; Bell: off; Prompting: on; Globbing: off	Displays debugging information.
Store unique: off; Receive unique: off	The name of the file on the FTP server is unique and the name of the local file is unique.
Case: off; CR stripping: on	Does not support obtaining multiple files once and deletes "\r" when downloading text files.
Ntrans: off	Does not use the input-output transmission table.
Nmap: off	The file name does not use the input-to-output mapping template.
Hash mark printing: off; Use of PORT cmds: on	Does not end with a pound sign (#) and uses "PORT" data transmission.

system

Use **system** to display the system information of the FTP server.

Syntax

system

Views

FTP client view

Predefined user roles

network-admin

Usage guidelines

You can perform this operation only after you log in to the FTP server.

Examples

Display the system information of the FTP server.

```
ftp> system
215 UNIX Type: L8
```

user

Use **user** to initiate an FTP authentication on the current FTP connection.

Syntax

user *username* [*password*]

Views

FTP client view

Predefined user roles

network-admin

Parameters

username: Specifies the username.

password: Specifies the password.

Usage guidelines

If you tried to access an FTP server but failed to pass the authentication, you can use this command to try again before the connection to the FTP server expires.

After you log in to an FTP server, you can initiate an FTP authentication to change to a new account. By changing to a new account, you can get a different privilege without re-establishing the FTP connection.

Make sure the specified username and password have been configured on the FTP server. If the username or password is not configured, this command fails and the FTP connection is closed.

Examples

After logging in to the FTP server, use username **ftp** and password **hello12345** to log in again to the FTP server.

- Method 1:

```
ftp> user ftp hello12345
331 Password required for ftp.
230 User logged in.
```

- Method 2:

```
ftp> user ftp
331 Password required for ftp.
Password:
230 User logged in.
```

verbose

Use **verbose** to enable or disable the device to display detailed information about FTP operations.

Syntax

verbose

Default

The device displays detailed information about FTP operations.

Views

FTP client view

Predefined user roles

network-admin

Usage guidelines

This command affects only the current FTP session.

Examples

Disable the device from displaying detailed information about FTP operations.

```
ftp> verbose
Verbose mode off.
```

Execute the **get** command.

```
ftp> get a.cfg 1.cfg
```

Enable the device to display detailed information about FTP operations.

```
ftp> verbose
Verbose mode on.
```

Execute the **get** command.

```
ftp> get a.cfg 2.cfg
227 Entering Passive Mode (192,168,1,58,68,14)
150-Accepted data connection
150 The computer is your friend. Trust the computer
226 File successfully transferred
3796 bytes received in 0.00762 seconds (486.5 kbyte/s)
```

TFTP commands

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

TFTP is not supported in FIPS mode.

tftp

Use **tftp** to download a file from a TFTP server or upload a file to a TFTP server in an IPv4 network.

Syntax

tftp *tftp-server* { **get** | **put** | **sget** } *source-filename* [*destination-filename*] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }] *

Views

User view

Predefined user roles

network-admin

Parameters

tftp-server: Specifies the IPv4 address or host name of a TFTP server. The host name can be a case-insensitive string of 1 to 253 characters and can contain only letters, digits, hyphens (-), underscores (_), and dots (.).

get: Downloads a file and writes the file directly to the destination folder. If the destination folder already has a file with the same name, the system deletes the existing file before starting the download operation. The existing file is permanently deleted even if the download operation fails.

put: Uploads a file.

sget: Downloads a file and saves the file to memory before writing it to the destination folder. The system starts to write the file to the destination folder only after the file is downloaded and saved to memory successfully. If the destination folder already has a file with the same name, the system overwrites the existing file. If the download or save-to-memory operation fails, the existing file in the destination folder is not overwritten.

source-filename: Specifies the source file name, a case-insensitive string of 1 to 1 to 255 characters.

destination-filename: Specifies the destination file name, a case-insensitive string of 1 to 255 characters. If this argument is not specified, the file uses the source file name.

dscp *dscp-value*: Specifies the DSCP value for IPv4 to use for outgoing TFTP packets to indicate the packet transmission priority. The value range is 0 to 63. The default is 0.

source { **interface** *interface-type interface-number* | **ip** *source-ip-address* }: Specifies the source address for outgoing TFTP packets. If you do not specify this option, the device uses the primary IPv4 address of the output interface for the route to the TFTP server as the source address.

- **interface** *interface-type interface-number*: Specifies an interface by its type and number. The device will use the interface's primary IPv4 address as the source IPv4 address. For successful TFTP packet transmission, make sure the interface is up and has the primary IPv4 address configured.

- **ip** *source-ip-address*: Specifies an IPv4 address. For successful TFTP packet transmission, make sure this address is the IPv4 address of an interface in up state on the device.

Usage guidelines

The source address specified with the **tftp** command takes precedence over the source address specified with the **tftp client source** command.

The source address specified with the **tftp client source** command applies to all TFTP connections. The source address specified with the **tftp** command applies only to the current TFTP connection.

Examples

Download the **new.bin** file from TFTP server 192.168.1.1 and save the file as **new.bin**.

```
<Sysname> tftp 192.168.1.1 get new.bin
Press CTRL+C to abort.
  % Total    % Received % Xferd  Average Speed   Time    Time     Time   Current
                                 Dload  Upload   Total   Spent    Left   Speed
100 13.9M  100 13.9M    0     0  1206k      0  0:00:11  0:00:11  --:--:-- 1206k
Writing file...Done.
<System>
```

Table 7 Command output

Field	Description
%	Percentage of file transmission progress.
Total	Size of files to be transmitted, in bytes.
%	Percentage of received file size to total file size.
Received	Received file size, in bytes.
%	Percentage of sent file size to total file size.
Xferd	Sent file size, in bytes.
Average Dload	Average download speed, in bps.
Speed Upload	Average upload speed, in bps.
Writing file…	The system was writing the downloaded file to the storage medium. This field is displayed only when the **get** or **sget** keyword is specified. If the operation succeeded, this command displays **Done** at the end of this field. If the operation failed, this command displays **Failed**.

Related commands

tftp client source

tftp client ipv6 source

Use **tftp client ipv6 source** to specify the source IPv6 address for TFTP packets sent to an IPv6 TFTP server.

Use **undo tftp client ipv6 source** to restore the default.

Syntax

tftp client ipv6 source { **interface** *interface-type interface-number* | **ipv6** *source-ipv6-address* }

undo tftp client ipv6 source

Default

No source address is specified for TFTP packets sent to an IPv6 TFTP server. The device selects a source IPv6 address as defined in RFC 3484.

Views

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. The device will use the interface's IPv6 address as the source address. For successful TFTP packet transmission, make sure the interface is up and is configured with an IPv6 address.

ipv6 *source-ipv6-address*: Specifies an IPv6 address . For successful TFTP packet transmission, make sure this address is the IPv6 address of an interface in up state on the device.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

The source address specified with the **tftp ipv6** command takes precedence over the source address specified with the **tftp client ipv6 source** command.

The source address specified with the **tftp client ipv6 source** command applies to all TFTP connections. The source address specified with the **tftp ipv6** command applies only to the TFTP connection that is being established.

Examples

Specify the source IPv6 address of 2000::1 for TFTP packets sent to an IPv6 TFTP server.

```
<Sysname> system–view
[Sysname] tftp client ipv6 source ipv6 2000::1
```

Related commands

tftp ipv6

tftp client source

Use **tftp client source** to specify the source IPv4 address for TFTP packets sent to an IPv4 TFTP server.

Use **undo tftp client source** to restore the default.

Syntax

tftp client source { **interface** *interface-type interface-number* | **ip** *source-ip-address* }

undo tftp client source

Default

No source IPv4 address is specified for TFTP packets sent to an IPv4 TFTP server. The device uses the primary IPv4 address of the output interface for the route to the server as the source address.

Views

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. The device will use the interface's primary IPv4 address as the source address. For successful TFTP packet transmission, make sure the interface is up and has the primary IPv4 address configured.

ip *source-ip-address*: Specifies an IPv4 address. For successful TFTP packet transmission, make sure this address is the IPv4 address of an interface in up state on the device.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

The source address specified with the **tftp** command takes precedence over the source address specified with the **tftp client source** command.

The source address specified with the **tftp client source** command applies to all TFTP connections. The source address specified with the **tftp** command applies only to the TFTP connection that is being established.

Examples

Specify the source IP address of 192.168.20.222 for TFTP packets sent to an IPv4 TFTP server.

```
<Sysname> system-view
[Sysname] tftp client source ip 192.168.20.222
```

Related commands

tftp

tftp ipv6

Use **tftp ipv6** to download a file from a TFTP server or upload a file to a TFTP server in an IPv6 network.

Syntax

tftp ipv6 *tftp-server* [**-i** *interface-type interface-number*] { **get** | **put** | **sget** } *source-filename* [*destination-filename*] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ipv6** *source-ipv6-address* }] *

Views

User view

Predefined user roles

network-admin

Parameters

tftp-server: Specifies the IPv6 address or host name of a TFTP server. The host name can be a case-insensitive string of 1 to 253 characters and can contain only letters, digits, hyphens (-), underscores (_), and dots (.).

-i *interface-type interface-number*: Specifies an output interface by its type and number. This option can be used only when the TFTP server address is a link local address and the specified

output interface has a link local address. For information about link local addresses, see *Layer 3—IP Services Configuration Guide*.

get: Downloads a file and writes the file directly to the destination folder. If the destination folder already has a file with the same name, the system deletes the existing file before starting the download operation. The existing file is permanently deleted even if the download operation fails.

put: Uploads a file.

sget: Downloads a file and saves the file to memory before writing it to the destination folder. The system starts to write the file to the destination folder only after the file is downloaded and saved to memory successfully. If the destination folder already has a file using the same name, the system overwrites the existing file. If the download or save-to-memory operation fails, the existing file in the destination folder is not overwritten.

source-filename: Specifies the source file name, a case-insensitive string of 1 to 255 characters.

destination-filename: Specifies the destination file name, a case-insensitive string of 1 to 255 characters. If this argument is not specified, the file uses the source file name.

dscp *dscp-value*: Specifies the DSCP value for IPv6 to use in outgoing TFTP packets to indicate the packet transmission priority. The value range is 0 to 63. The default is 0.

source { **interface** *interface-type interface-number* | **ipv6** *source-ipv6-address* }: Specifies the source address for outgoing TFTP packets. If you do not specify this option, the device selects a source IPv6 address as defined in RFC 3484.

- **interface** *interface-type interface-number*: Specifies an interface by its type and number. The device will use the interface's IPv6 address as the source IPv6 address. For successful TFTP packet transmission, make sure the interface is up and is configured with an IPv6 address.
- **ipv6** *source-ipv6-address*: Specifies an IPv6 address. For successful TFTP packet transmission, make sure this address is the IPv6 address of an interface in up state on the device.

Usage guidelines

The source address specified with the **tftp ipv6** command takes precedence over the source address specified with the **tftp client ipv6 source** command.

The source address specified with the **tftp client ipv6 source** command applies to all TFTP connections. The source address specified with the **tftp ipv6** command applies only to the current TFTP connection.

Examples

Download the **new.bin** file from TFTP server 2001::1 and save the file as **new.bin**.

```
<Sysname> tftp ipv6 2001::1 get new.bin new.bin
Press CTRL+C to abort.
   % Total    % Received % Xferd  Average Speed   Time    Time     Time   Current
                                  Dload  Upload   Total   Spent    Left   Speed
100 13.9M  100 13.9M    0     0  1206k      0  0:00:11  0:00:11  --:--:-- 1206k
Writing file...Done.
```

For more information about the command output, see Table 7.

tftp-server acl

Use **tftp-server acl** to use an ACL to control the device's access to TFTP servers in an IPv4 network.

Use **undo tftp-server acl** to restore the default.

Syntax

tftp-server acl *acl-number*

undo tftp-server acl

Default

No ACL is used to control the device's access to TFTP servers.

Views

System view

Predefined user roles

network-admin

Parameters

acl-number: Specifies the number of a basic ACL, in the range of 2000 to 2999.

Usage guidelines

You can use an ACL to deny or permit the device's access to specific TFTP servers.

Examples

Allow the device to access only TFTP server 1.1.1.1.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule permit source 1.1.1.1 0
[Sysname-acl-ipv4-basic-2000] quit
[Sysname] tftp-server acl 2000
```

tftp-server ipv6 acl

Use **tftp-server ipv6 acl** to use an ACL to control the device's access to TFTP servers in an IPv6 network.

Use **undo tftp-server ipv6 acl** to restore the default.

Syntax

tftp-server ipv6 acl *ipv6-acl-number*

undo tftp-server ipv6 acl

Default

No ACL is used to control the device's access to TFTP servers.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies the number of a basic ACL, in the range of 2000 to 2999.

Usage guidelines

You can use an ACL to deny or permit the device's access to specific TFTP servers.

Examples

Allow the device to access only TFTP server 2001::1.

```
<Sysname> System-view
[Sysname] acl ipv6 basic 2001
[Sysname-acl-ipv6-basic-2001] rule permit source 2001::1/128
[Sysname-acl-ipv6-basic-2001] quit
[Sysname] tftp-server ipv6 acl 2001
```

Contents

File system management commands

IMPORTANT:

- Before managing storage media, file systems, directories, and files, make sure you know the possible impact.
- A file or directory whose name starts with a dot character (.) is a hidden file or directory. To prevent the system from hiding a file or directory, make sure the file or directory name does not start with a dot character.
- Some system files and directories are hidden. For correct system operation and full functionality, do not modify or delete hidden files or directories.

File system names, directory names, and file names must be compliant with the naming conventions. For more information about the naming conventions and the methods for specifying the names, see file system management in *Fundamentals Configuration Guide*.

Before you use the **copy**, **delete**, **fixdisk**, **format**, **gunzip**, **gzip**, **mkdir**, **move**, **rename**, **rmdir**, or **undelete** command on a file system, make sure the file system is not write protected.

You cannot access a storage medium that is being partitioned, or a file system that is being formatted or repaired. To access the file system, wait for the ongoing operation to be completed and then use one of the following methods:

- Use the absolute path to specify a file or directory. For example, use the **dir flash:/** command to display the files and directories in the **flash:** file system.
- Use the **cd** command to change the working directory to the root directory of the file system before accessing a file or directory in the file system. For example, to display the files and directories in the root directory of the **flash:** file system, perform the following tasks:
  a. Use the **cd flash:/** command to change the working directory to the root directory of the file system.
  b. Execute the **dir** command.

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

cd

Use **cd** to change the working directory.

Syntax

cd { *directory* | **..** }

Views

User view

Predefined user roles

network-admin

Parameters

directory: Specifies the destination directory.

..: Specifies the parent directory. If the working directory is the root directory, an error message appears when you execute the **cd ..** command. No online help information is available for this keyword.

Examples

Access the **test** directory after logging in to the device.

```
<Sysname> cd test
```

Change to the parent directory.

```
<Sysname> cd ..
```

copy

Use **copy** to copy a file.

Syntax

In non-FIPS mode:

copy *source-file* { *dest-file* | *dest-directory* } [**source interface** *interface-type interface-number*]

In FIPS mode:

copy *source-file* { *dest-file* | *dest-directory* }

Views

User view

Predefined user roles

network-admin

Parameters

source-file: Specifies the name or URL of the file to be copied in non-FIPS mode, and specifies the name of the file to be copied in FIPS mode. If the file resides on a remote file server rather than on the device, specify the URL of the file. Whether a URL is case sensitive depends on the server.

dest-file: Specifies the name or URL for the destination file in non-FIPS mode, and specifies the name for the destination file in FIPS mode. To copy the source file to a remote file server, specify a URL. Whether a URL is case sensitive depends on the server.

dest-directory: Specifies the destination directory or URL in non-FIPS mode, and specifies the destination directory in FIPS mode. To copy the source file to a remote file server, specify a URL. The device copies the source file to the destination location and saves the file with its original file name. Whether a URL is case sensitive depends on the server.

source interface *interface-type interface-number*: Specifies the source interface used to connect to the server. After you specify the source interface, the device uses the primary IP address of the source interface as the source IP address for outgoing packets. If you do not specify this option, the device uses the outgoing interface as the source interface.

Usage guidelines

In FIPS mode, the **copy** command can only copy a local file and save it locally.

In non-FIPS mode, you can use the **copy** command to perform the following tasks:

- Copy a local file and save it locally.
- Copy a local file and save it to an FTP, TFTP, or HTTP server.
- Copy a file from an FTP, TFTP, or HTTP server and save it locally.

To specify a file or directory, use the following guidelines:

Location	Name format	Remarks
On the device	Use the file name guidelines in *Fundamentals Configuration Guide*.	N/A
On an FTP server	Enter the URL in the format of **ftp://***FTP username*[**:***password*]*@server address*[**:***port number*]**/***file path*[**/***file name*].	The username and password must be the same as the username and password configured on the FTP server. If the server authenticates users only by the username, you are not required to enter the password. For example, to use the username a and password 1 and specify the startup.cfg file in the authorized working directory on the FTP server 1.1.1.1, enter ftp://a:1@1.1.1.1/startup.cfg.
On a TFTP server	Enter the URL in the format of **tftp://***server address*[**:***port number*]**/***file path*[**/***file name*].	For example, to specify the startup.cfg file in the working directory on TFTP server 1.1.1.1, enter the URL tftp://1.1.1.1/startup.cfg.
On an HTTP server	Enter the URL in the format of **http://**[*HTTP username*[**:***password*]@]*server address*[**:***port number*]**/***filepath*[**/***file name*].	The username and password in the URL must be the same as the username and password configured on the server. If only the username is required for authentication, you do not need to enter the password. If authentication is not required, you do not need to enter the username or password. For example, the **startup.cfg** file is saved in the authorized directory on the HTTP server at 1.1.1.1. The HTTP account username and password are **a** and **1**, respectively. To copy the file, enter the URL http://a:1@1.1.1.1/startup.cfg. If authentication is not required, enter the URL http://1.1.1.1/startup.cfg.

To specify an IPv6 address, enclose the IPv6 address in square brackets ([ ]), for example, ftp://test:test@[2001::1]:21/test.cfg.

Examples

Copy the **test.cfg** file in the current directory and save it to the current directory as **testbackup.cfg**.

```
<Sysname> copy test.cfg testbackup.cfg
Copy flash:/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file flash:/test.cfg to flash:/testbackup.cfg...Done.
```

Copy the **1.cfg** file from the **flash:** file system's **test** directory to the USB disk. Save the copy to the **testbackup** directory on the first partition as **1backup.cfg**.

```
<Sysname> copy flash:/test/1.cfg usba0:/testbackup/1backup.cfg
Copy flash:/test/1.cfg to usba0:/testbackup/1backup.cfg? [Y/N]:y
Copying file flash:/test/1.cfg to usba0:/testbackup/1backup.cfg...Done.
```

Copy the **test.cfg** file in the current directory and save it to the root directory of a file system in a specific slot as **testbackup.cfg**.

```
<Sysname> copy test.cfg slot2#flash:/
Copy flash:/test.cfg to slot2#flash:/test.cfg? [Y/N]:y
Copying file flash:/test.cfg to slot2#flash:/test.cfg...Done.
```

Copy **test.cfg** from the working directory on FTP server 1.1.1.1. Save the copy to the local current directory as **testbackup.cfg.** The FTP username is **user**. The password is **private**.

```
<Sysname> copy ftp://user:private@1.1.1.1/test.cfg testbackup.cfg
Copy ftp://user:private@1.1.1.1/test.cfg to flash:/testbackup.cfg? [Y/N]:y
```

```
Copying file ftp://user:private@1.1.1.1/test.cfg to flash:/testbackup.cfg... Done.
```

Copy **test.cfg** from the current directory. Save the copy to the working directory on FTP server 1.1.1.1 as **testbackup.cfg**. The FTP username is **user**. The password is **private**.

```
<Sysname> copy test.cfg ftp://user:private@1.1.1.1/testbackup.cfg
Copy flash:/test.cfg to ftp://user:private@1.1.1.1/testbackup.cfg? [Y/N]:y
Copying file flash:/test.cfg to ftp://user:private@1.1.1.1/testbackup.cfg... Done.
```

Copy **test.cfg** from the working directory on TFTP server 1.1.1.1. Save the copy to the local current directory as **testbackup.cfg**.

```
<Sysname> copy tftp://1.1.1.1/test.cfg testbackup.cfg
Copy tftp://1.1.1.1/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file tftp://1.1.1.1/test.cfg to flash:/testbackup.cfg... Done.
```

Copy **test.cfg** from the current directory. Save the copy to the working directory on TFTP server 1.1.1.1 as **testbackup.cfg**.

```
<Sysname> copy test.cfg tftp://1.1.1.1/testbackup.cfg
Copy flash:/test.cfg to tftp://1.1.1.1/testbackup.cfg? [Y/N]:y
Copying file flash:/test.cfg to tftp://1.1.1.1/testbackup.cfg... Done.
```

Copy **test.cfg** from the working directory on FTP server 2001::1. Save the copy to the local current directory as **testbackup.cfg**. The FTP username is **user**. The password is **private**.

```
<Sysname> copy ftp://user:private@[2001::1]/test.cfg testbackup.cfg
Copy ftp://user:private@[2001::1]/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file ftp://user:private@[2001::1]/test.cfg to flash:/testbackup.cfg... Done.
```

Copy **test.cfg** from the working directory on TFTP server 2001::1. Save the copy to the local current directory as **testbackup.cfg**.

```
<Sysname> copy tftp://[2001::1]/test.cfg testbackup.cfg
Copy tftp://[2001::1]/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file tftp://[2001::1]/test.cfg to flash:/testbackup.cfg... Done.
```

Copy **test.cfg** from the authorized directory on HTTP server 1.1.1.1. Save the copy to the local current directory as **testbackup.cfg**. The HTTP login username is **user**. The password is **private**.

```
<Sysname> copy http://user:private@1.1.1.1/test.cfg testbackup.cfg
Copy http://user:private@1.1.1.1/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file http://user:private@1.1.1.1/test.cfg to flash:/testbackup.cfg... Done.
```

Copy **test.cfg** from the current directory. Save the copy to the authorized directory on HTTP server 1.1.1.1 as **testbackup.cfg**. The HTTP login username is **user**. The password is **private**.

```
<Sysname> copy test.cfg http://user:private@1.1.1.1/testbackup.cfg
Copy flash:/test.cfg to http://user:private@1.1.1.1/testbackup.cfg? [Y/N]:y
Copying file flash:/test.cfg to http://user:private@1.1.1.1/testbackup.cfg... Done.
```

Copy **test.cfg** from the authorized directory on HTTP server 2001::1. Save the copy to the local current directory as **testbackup.cfg**. The HTTP login username is **user**. The password is **private**.

```
<Sysname> copy http://user:private@[2001::1]/test.cfg testbackup.cfg
Copy http://user:private@[2001::1]/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file http://user:private@[2001::1]/test.cfg to flash:/testbackup.cfg... Done.
```

delete

Use **`delete`** to delete a file.

Syntax

`delete` [**`/unreserved`**] *`file`*

Views

User view

Predefined user roles

network-admin

Parameters

/unreserved: Permanently deletes the specified file. If you do not specify this keyword, the command moves the file to the recycle bin.

file: Specifies the name of the file to be deleted. Asterisks (*) are acceptable as wildcards. For example, to remove files with the **.txt** extension in the current directory, enter **delete *.txt**.

Usage guidelines

CAUTION:

The **delete /unreserved** *file* command deletes a file permanently. The file cannot be restored.

The **delete** *file* command (without **/unreserved**) moves a file to the recycle bin. A file moved to the recycle bin can be restored by using the **undelete** command.

Do not use the **delete** command to delete files from the recycle bin. To delete files from the recycle bin, use the **reset recycle-bin** command.

If you delete two files that have the same name from different directories, both files are retained in the recycle bin. If you successively delete two files that have the same name from the same directory, only the most recently deleted file is retained in the recycle bin.

Examples

Remove the **1.cfg** file from the current directory.

```
<Sysname> delete 1.cfg
Delete flash:/1.cfg? [Y/N]:y
Deleting file flash:/1.cfg...Done.
```

Permanently delete the **1.cfg** file from the current directory.

```
<Sysname> delete /unreserved 1.cfg
The file cannot be restored. Delete flash:/1.cfg? [Y/N]:y
Deleting the file permanently will take a long time. Please wait...
Deleting file flash:/1.cfg...Done.
```

Related commands

reset recycle-bin

undelete

dir

Use **dir** to display files or directories.

Syntax

dir [**/all**] [*file* | *directory* | **/all-filesystems**]

Views

User view

Predefined user roles

network-admin

Parameters

/all: Displays all files and directories in the current directory, visible or hidden. If you do not specify this option, only visible files and directories are displayed.

file: Displays a specific file. This argument can use the asterisk (*) as a wildcard. For example, to display files with the **.txt** extension in the current directory, enter **dir *.txt**.

directory: Displays a specific directory.

/all-filesystems: Displays files and directories in the root directories of all file systems on the device.

Usage guidelines

If no option is specified, the command displays all visible files and directories in the current directory.

The directory name of the recycle bin is **.trash**. To display files in the recycle bin, use either of the following methods:

- Execute the **dir /all .trash** command.
- Execute the **cd .trash** command and then the **dir** command.

If multiple users perform file operations (for example, creating or deleting files or directories) at the same time, the output for this command might be incorrect.

Examples

Display information about all files and directories in the current directory.

```
<Sysname> dir /all
Directory of flash:/
...
```

Display files and directories in the root directories of all file systems on the device.

```
<Sysname> dir /all-filesystems
Directory of flash:/
...

Directory of usba0:/
...
```

Table 1 Command output

Field	Description
Directory of	Current directory.

Field	Description
0 -rwh 3144 Apr 26 2014 13:45:28 xx.xx	File or directory information: • **0**—File or directory number, which is automatically allocated by the system. • **-rwh**—Attributes of the file or directory. The first character is the directory indicator (**d** for directory and **–** for file). The second character indicates whether the file or directory is readable (**r** for readable). The third character indicates whether the file or directory is writable (**w** for writable). The fourth character indicates whether the file or directory is hidden (**h** for hidden, **-** for visible). Modifying, renaming, or deleting hidden files might affect functions. • **3144**—File size in bytes. For a directory, a hyphen (-) is displayed. • **Apr 26 2014 13:45:28**—Last date and time when the file or directory was modified. • **xx.xx**—File or directory name.

execute

Use **`execute`** to execute a batch file.

Syntax

`execute` *`filename`*

Views

System view

Predefined user roles

network-admin

Parameters

`filename:` Specifies the name of a batch file.

Usage guidelines

A batch file contains a set of commands. Executing a batch file executes the commands in the file one by one.

To execute a batch file on the device, create a batch file on a PC and load the batch file to the device.

As a best practice, try every command on the device to make sure the command can be executed correctly before adding the command to a batch file. If a command is invalid or a condition for executing the command is not met, the command fails and the system continues to execute the next command.

When executing an interactive command in a batch file, the system uses the default inputs.

Examples

Execute batch file **test.bat**.

```
<Sysname> fdisk usba: 3
[Sysname] execute test.bat
```

fdisk

Use **`fdisk`** to partition a storage medium.

Syntax

`fdisk` *`medium`* [*`partition-number`*]

Views

User view

Predefined user roles

network-admin

Parameters

medium: Specifies the name of the storage medium to be partitioned.

partition-number: Specifies the number of partitions, in the range of 1 to 4. If you specify this argument, the storage medium is divided evenly into the specified number of partitions. To customize the sizes of partitions, do not provide this argument.

Usage guidelines

The flash memory cannot be partitioned. A partition cannot be partitioned.

Before partitioning a storage medium, perform the following tasks:

- Back up the files in the storage medium. The partition operation clears all data on the medium.
- Make sure no other users are accessing the medium.
- Make sure the storage medium to be partitioned is not write protected. If the storage medium is write protected, the operation will fail, and you must remount or reinstall the storage medium to restore access to the storage medium.

After partitioning a storage medium, you must format the partitions to create the file systems before you can access the file systems.

The actual partition size and the specified partition size might have a difference of less than 5% of the storage medium's total size.

To change the sizes of partitions on a storage medium, partition the storage medium again and specify the required sizes for the partitions.

Before removing a partitioned storage medium, you must unmount all file systems on the storage medium.

Examples

Divide the USB disk on the device evenly into three partitions.

```
<Sysname> fdisk usba: 3
Capacity of usba: : 256M bytes
usba: will be divided into the following partitions:
DeviceName      Capacity
usba0:            85MB
usba1:            85MB
usba2:            86MB
All data on usba: will be lost, continue? [Y/N]:y
Partitioning usba:...Done.
```

Divide the USB disk on the device into one partition.

```
<Sysname> fdisk usba:
The capacity of usba: : 256M bytes
Partition 1 (32MB~224MB, 256MB. Press CTRL+C to quit or Enter to use all available space):
```

// Press **Enter** or enter **256.**

```
usba: will be divided into the following partition(s):
DeviceName    Capacity
usba0:          256MB
All data on usba: will be lost, continue? [Y/N]:y
```

```
Partitioning usba:...Done.
```

Divide the USB disk on the device into three partitions and specify the size for each partition.

```
<Sysname> fdisk usba:
The capacity of usba: : 256M bytes
Partition 1 (32MB~224MB, 256MB, Press CTRL+C to quit or Enter to use all available
space):128
```

// Enter **128** to set the size of the first partition to 128 MB.

```
Partition 2 (32MB~96MB, 128MB, Press CTRL+C to quit or Enter to use all available space):31
```

// Enter **31** to set the size of the second partition to 31 MB.

```
The partition size must be greater than or equal to 32MB.
Partition 2 (32MB~96MB, 128MB, Press CTRL+C to quit or Enter to use all available
space):1000
```

// Enter **1000** to set the size of the second partition to 1000 MB.

```
The partition size must be less than or equal to 128MB.
Partition 2 (32MB~96MB, 128MB, Press CTRL+C to quit or Enter to use all available space):127
```

// Enter **127** to set the size of the second partition to 127 MB.

```
The remaining space is less than 32MB. Please enter the size of partition 2 again.
Partition 2 (32MB~96MB, 128MB, Press CTRL+C to quit or Enter to use all available space):56
```

// Enter **56** to set the size of the second partition to 56 MB.

```
Partition 3 (32MB~40MB, 72MB, Press CTRL+C to quit or Enter to use all available space):
```

// Press **Enter** to assign the remaining space to the third partition.

```
usba: will be divided into the following partition(s):
DeviceName     Capacity
usba0:            128MB
usba1:            56MB
usba2:            72MB
All data on usba: will be lost, continue? [Y/N]:y
Partitioning usba:...Done.
```

file prompt

Use **file prompt** to set the operation mode for files and directories.

Use **undo file prompt** to restore the default.

Syntax

file prompt { **alert** | **quiet** }

undo file prompt

Default

The operation mode is **alert**. The system prompts for confirmation when you perform a destructive file or directory operation.

Views

System view

Predefined user roles

network-admin

Parameters

alert: Prompts for confirmation when a destructive file or directory operation is being performed.

quiet: Gives no confirmation prompt for file or directory operations except the recycle bin emptying operation.

Usage guidelines

In quiet mode, the system does not prompt for confirmation when a user performs a file or directory operation except the recycle bin emptying operation. The **alert** mode provides an opportunity to cancel a disruptive operation.

Examples

Set the file and directory operation mode to **alert**.

```
<Sysname> system-view
[Sysname] file prompt alert
```

fixdisk

Use **fixdisk** to check a file system for damage and repair any damage.

Syntax

fixdisk *filesystem*

Views

User view

Predefined user roles

network-admin

Parameters

filesystem: Specifies the name of a file system.

Usage guidelines

Use this command to fix a file system when space in the file system cannot be used or released.

You can repair a file system only when no other users are accessing the file system.

Examples

Repair file system **flash:**.

```
<Sysname> fixdisk flash:
Restoring flash: may take some time...
Restoring flash:...Done.
```

format

Use **format** to format a file system.

Syntax

format *filesystem*

Views

User view

Predefined user roles

network-admin

Parameters

filesystem: Specifies the name of a file system.

Usage guidelines

CAUTION:

Formatting a file system permanently deletes all files and directories in the file system. You cannot restore the deleted files or directories. If a startup configuration file exists in the file system, back up the file if necessary.

The device requires that the file systems on hot swappable storage media be VFAT file systems. To use a file system of a different type on the device, you must use this command to format the file system.

You can format a file system only when no other users are accessing the file system.

A file system to be formatted cannot contain security log files. Only a user with the security-audit user role can delete security log files. For more information about the security-audit user role, see RBAC in *Fundamentals Configuration Guide*.

Examples

Format file system **flash:**.

```
<Sysname> format flash:
All data on flash: will be lost, continue? [Y/N]:y
Formatting flash:... Done.
```

Format the file system on the third partition of the USB disk.

```
<Sysname> format usba2:
All data on usba2: will be lost, continue? [Y/N]:y
Formatting usba2:... Done.
```

gunzip

Use **gunzip** to decompress a file.

Syntax

gunzip *file*

Views

User view

Predefined user roles

network-admin

Parameters

file: Specifies the name of the file to be decompressed. This argument must use the **.gz** extension.

Usage guidelines

This command deletes the specified file after decompressing it.

Examples

Decompress file **system.bin.gz**:

1. Before decompressing the file, you can display files whose names start with the **system.** string.

```
<Sysname> dir system.*
Directory of flash:
   1 -rw-          20 Jun 14 2012 10:18:53   system.bin.gz
```

```
251904 KB total (193312 KB free)
```

2. Decompress the file **system.bin.gz**.

```
<Sysname> gunzip system.bin.gz
Decompressing file flash:/system.bin.gz..... Done.
```

3. Verify the decompress operation.

```
<Sysname> dir system.*
Directory of flash:
   1 -rw-           0 May 30 2012 11:42:25   system.bin


251904 KB total (193312 KB free)
```

gzip

Use **gzip** to compress a file.

Syntax

gzip *file*

Views

User view

Predefined user roles

network-admin

Parameters

file: Specifies the name of the file to be compressed.

Usage guidelines

This command saves the compressed file to the *file***.gz** file and deletes the source file.

Examples

Compress file **system.bin**:

1. Before compressing the file, you can display files whose names start with the **system.** string.

```
<Sysname> dir system.*
Directory of flash:
   1 -rw-           0 May 30 2012 11:42:24   system.bin


1251904 KB total (193312 KB free)
```

2. Compress the file **system.bin**.

```
<Sysname> gzip system.bin
Compressing file flash:/system.bin..... Done.
```

3. Verify the compress operation.

```
<Sysname> dir system.*
Directory of flash:
   1 -rw-          20 Jun 14 2012 10:18:53   system.bin.gz
```

```
251904 KB total (193312 KB free)
```

md5sum

Use **md5sum** to use the MD5 algorithm to calculate the digest of a file.

Syntax

md5sum *file*

Views

User view

Predefined user roles

network-admin

network-operator

Parameters

file: Specifies the name of a file.

Usage guidelines

You can use file digests to verify file integrity.

Examples

Use the MD5 algorithm to calculate the digest of file **system.bin**.

```
<Sysname> md5sum system.bin
MD5 digest:
4f22b6190d151a167105df61c35f0917
```

mkdir

Use **mkdir** to create a directory.

Syntax

mkdir *directory*

Views

User view

Predefined user roles

network-admin

Parameters

directory: Specifies a directory.

Usage guidelines

The name of the directory to be created must be unique in the parent directory.

You can create a directory only in an existing directory. For example, to create the **flash:/test/mytest** directory, make sure the **test** directory already exists.

Examples

Create the **test** directory in the current directory.

```
<Sysname> mkdir test
Creating directory flash:/test... Done.
```

Create the **test/subtest** directory in the current directory.

```
<Sysname> mkdir test/subtest
Creating directory flash:/test/subtest... Done.
```

more

Use **more** to display the contents of a text file.

Syntax

more *file*

Views

User view

Predefined user roles

network-admin

Parameters

file: Specifies the name of a file.

Examples

Display the contents of the **test.txt** file.

```
<Sysname> more test.txt
Have a nice day.
```

Display the contents of the **testcfg.cfg** file.

```
<Sysname> more testcfg.cfg

#
 version 7.1.070, Release 1201
#
 sysname Sysname
#
vlan 2
#
return
<Sysname>
```

mount

Use **mount** to mount a file system.

Syntax

mount *filesystem*

Views

User view

Predefined user roles

network-admin

Parameters

filesystem: Specifies the name of a file system.

Usage guidelines

Generally, file systems on a hot-swappable storage medium are automatically mounted when the storage medium is connected to the device. If the system cannot recognize a file system, however, you must mount the file system before you can access it.

To avoid file system corruption, do not perform the following tasks while the system is mounting a file system:

- Reboot, power cycle, or power off the device.
- Install or remove storage media.
- Perform a switchover.

To remove a hot-swappable storage medium from the device, you must first unmount all file systems on the storage medium. Removing a mounted hot-swappable storage medium might damage files on the storage medium or even the storage medium.

Examples

Mount a file system on the USB disk.

```
<Sysname> mount usba0:
```

Related commands

umount

move

Use **move** to move a file.

Syntax

move *source-file* { *dest-file* | *dest-directory* }

Views

User view

Predefined user roles

network-admin

Parameters

source-file: Specifies the name of the source file.

dest-file: Specifies the name of the destination file.

dest-directory: Specifies the name of the destination directory.

Usage guidelines

If you specify a destination directory, the system moves the source file to the specified directory without changing the file name.

Examples

Move the **flash:/test/sample.txt** file to **flash:/**, and save it as **1.txt**.

```
<Sysname> move test/sample.txt 1.txt
Move flash:/test/sample.txt to flash:/1.txt? [Y/N]:y
Moving file flash:/test/sample.txt to flash:/1.txt ...Done.
```

Move the **b.cfg** file to the **test2** directory.

```
<Sysname> move b.cfg test2
Move flash:/b.cfg to flash:/test2/b.cfg? [Y/N]:y
Moving file flash:/b.cfg to flash:/test2/b.cfg... Done.
```

pwd

Use **pwd** to display the working directory.

Syntax

pwd

Views

User view

Predefined user roles

network-admin

Examples

Display the working directory.

```
<Sysname> pwd
flash:
```

rename

Use **rename** to rename a file or directory.

Syntax

rename { *source-file* | *source-directory* } { *dest-file* | *dest-directory* }

Views

User view

Predefined user roles

network-admin

Parameters

source-file: Specifies the name of the source file.

source-directory: Specifies the name of the source directory.

dest-file: Specifies the name of the destination file.

dest-directory: Specifies the name of the destination directory.

Usage guidelines

This command is not executed if the destination file or directory name is already used by an existing file or directory in the working directory.

Examples

Rename the **copy.cfg** file as **test.cfg**.

```
<Sysname> rename copy.cfg test.cfg
Rename flash:/copy.cfg as flash:/test.cfg? [Y/N]:y
Renaming flash:/copy.cfg as flash:/test.cfg... Done.
```

reset recycle-bin

Use **reset recycle-bin** to delete files from the recycle bin.

Syntax

reset recycle-bin [**/force**]

Views

User view

Predefined user roles

network-admin

Parameters

/force: Deletes all files in the recycle bin without prompting for confirmation. If you do not specify this option, the command prompts you to confirm the deletion operation for each file.

Usage guidelines

CAUTION:

The files in a recycle bin can be restored by using the **undelete** command. If you delete a file from the recycle bin, that file cannot be restored. Before you delete files from a recycle bin, make sure the files are no longer in use.

The **delete** *file* command only moves a file to the recycle bin. To permanently delete the file, use the **reset recycle-bin** command to delete the file from the recycle bin.

Examples

Empty the recycle bin. (In this example there are two files in the recycle bin.)

```
<Sysname> reset recycle-bin
Clear flash:/a.cfg? [Y/N]:y
Clearing file flash:/a.cfg... Done.
Clear flash:/b.cfg? [Y/N]:y
Clearing file flash:/b.cfg... Done.
```

Delete the **b.cfg** file from the recycle bin. (In this example there are two files in the recycle bin.)

```
<Sysname> reset recycle-bin
Clear flash:/a.cfg? [Y/N]:n
Clear flash:/b.cfg? [Y/N]:y
Clearing file flash:/b.cfg... Done.
```

Related commands

delete

rmdir

Use **rmdir** to delete a directory.

Syntax

rmdir *directory*

Views

User view

Predefined user roles

network-admin

Parameters

directory: Specifies a directory.

Usage guidelines

CAUTION:

To delete a directory, you must first delete all files and subdirectories in the directory permanently or move them to the recycle bin. If you move them to the recycle bin, executing the **rmdir** command to delete the directory will delete them permanently. Before you use the **rmdir** command to delete a directory, you must make sure the directory and its files and subdirectories are no longer in use.

Examples

Delete the **subtest** directory.

```
<Sysname>rmdir subtest/
Remove directory flash:/test/subtest and the files in the recycle-bin under this directory
will be deleted permanently. Continue? [Y/N]:y
Removing directory flash:/test/subtest... Done.
```

sha256sum

Use **sha256sum** to use the SHA-256 algorithm to calculate the digest of a file.

Syntax

sha256sum *file*

Views

User view

Predefined user roles

network-admin

Parameters

file: Specifies the name of a file.

Usage guidelines

You can use file digests to verify file integrity.

Examples

Use the SHA-256 algorithm to calculate the digest of file **system.bin**.

```
<Sysname> sha256sum system.bin
SHA256 digest:
0851e0139f2770e87d01ee8c2995ca9e59a8f5f4062e99af14b141b1a36ca152
```

tar create

Use **tar create** to archive files and directories.

Syntax

tar create [**gz**] **archive-file** *dest-file* [**verbose**] **source** { *source-file* | *source-directory* }&<1-5>

Views

User view

Predefined user roles

network-admin

Parameters

gz: Uses gzip to compress the files and directories before archiving them. If you do not specify this keyword, the command archives the files and directories without compressing them.

archive-file *dest-file*: Specifies the archive file name. If you specified the **gz** keyword, the extension of the archive file name must be **.tar.gz**. If you did not specify the **gz** keyword, the extension of the archive file name must be **.tar**.

verbose: Displays the names of the successfully archived files and directories. If you do not specify this keyword, the command does not display the names of the successfully archived files and directories.

source { *source-file* | *source-directory* }&<1-5>: Specifies the files and directories to be archived. The argument can be a space-separated list of up to five items. Each item can be a file or directory name.

Examples

Archive the **1.cfg** and **2.cfg** files and the **test** directory to **a.tar**.

```
<Sysname> tar create archive-file a.tar source 1.cfg 2.cfg test
Creating archive flash:/a.tar Done.
```

Compress and archive the **1.cfg** and **2.cfg** files and the **test** directory to **b.tar.gz**.

```
<Sysname> tar create gz archive-file b.tar.gz source 1.cfg 2.cfg test
Creating archive flash:/b.tar.gz Done.
```

Compress and archive files and directories, and display the successfully archived files and directories.

```
<Sysname> tar create gz archive-file c.tar.gz verbose source 1.cfg 2.cfg test
1.cfg
2.cfg
test/
test/a.log
test/subtest/
test/subtest/aa.log
```

Related commands

tar extract

tar list

tar extract

Use **tar extract** to extract files and directories.

Syntax

tar extract archive-file *file* [**verbose**] [**screen** | **to** *directory*]

Views

User view

Predefined user roles

network-admin

Parameters

`archive-file` *`file`*: Specifies the archive file name. The extension can be **.tar** or **.tar.gz**.

`verbose`: Displays the names of the successfully extracted files and directories.

`screen`: Displays the content of the extracted files and directories on the screen. The extracted files are not saved.

`to` *`directory`*: Saves the extracted files and directories to a different directory. The *`directory`* argument specifies the directory.

Usage guidelines

IMPORTANT:

Before specifying the **`screen`** keyword for this command, use the **`tar list`** command to identify the types of the archived files. As a best practice, specify the keyword only if all archived files are text files. Displaying the content of an archived non-text file that contains terminal control characters might result in garbled characters and even cause the terminal unable to operate correctly. To use the terminal again, you must close the current connection and log in to the device again.

If you do not specify the **`screen`** keyword or the **`to`** *`directory`* option, the command saves the extracted files and directories to the working directory.

The command saves the extracted files and directories by using their original names. If a file or directory that has the same name as an extracted file or directory already exists in the destination directory, the file or directory is overwritten.

Examples

Extract files and directories from archive file **a.tar**.

```
<Sysname> tar extract archive-file a.tar
Extracting archive flash:/a.tar Done.
```

Extract files and directories from archive file **a.tar**, and display the names of the successfully extracted files and directories.

```
<Sysname> tar extract archive-file b.tar.gz verbose
1.cfg
2.cfg
test/
test/a.log
test/subtest/
test/subtest/aa.log
```

Extract files and directories from archive file **a.tar**, and display the content of the files on the screen.

```
<Sysname> tar extract archive-file c.tar.gz screen
#
 version 7.1.070, Release 1201
#
 sysname Sysname
#
...
```

Related commands

`tar create`

`tar list`

tar list

Use **tar list** to display the names of archived files and directories.

Syntax

tar list archive-file *file*

Views

User view

Predefined user roles

network-admin

Parameters

archive-file *file*: Specifies the archive file name. The extension can be **.tar** or **.tar.gz**.

Examples

Display the names of archived files and directories.

```
<Sysname> tar list archive-file a.tar
1.cfg
2.cfg
test/
test/a.log
test/subtest/
test/subtest/aa.log
```

Related commands

tar create

tar extract

umount

Use **umount** to unmount a file system.

Syntax

umount *filesystem*

Views

User view

Predefined user roles

network-admin

Parameters

filesystem: Specifies the name of a file system.

Usage guidelines

File systems on a storage medium are automatically mounted when the storage medium is connected to the device. To remove a hot-swappable storage medium from the device, you must first unmount all file systems on the storage medium. Removing a mounted hot-swappable storage medium might damage files on the storage medium or even the storage medium.

You can unmount a file system only when no other users are accessing the file system.

To avoid file system corruption, do not perform the following tasks while the system is unmounting a file system:

- Reboot, power cycle, or power off the device.
- Install, remove, or access storage media.
- Perform a switchover.

Examples

Unmount a file system on a USB disk.

```
<Sysname> umount usba0:
```

Related commands

mount

undelete

Use **undelete** to restore a file from the recycle bin.

Syntax

undelete *file*

Views

User view

Predefined user roles

network-admin

Parameters

file: Specifies the name of the file to be restored.

Usage guidelines

If a file with the same name already exists in the directory, the system prompts whether or not you want to overwrite the existing file. If you enter **Y**, the existing file is overwritten. If you enter **N**, the command is not executed.

Examples

Restore the **copy.cfg** file, which was moved from the root directory of the **flash:** file system to the recycle bin.

```
<Sysname>undelete copy.cfg
Undelete flash:/copy.cfg? [Y/N]:y
Undeleting file flash:/copy.cfg... Done.
```

Restore the **startup.cfg** file, which was moved from the **flash:/seclog** directory to the recycle bin.

- Method 1:

  ```
  <Sysname>undelete seclog/startup.cfg
  Undelete flash:/seclog/startup.cfg? [Y/N]:y
  Undeleting file flash:/seclog/startup.cfg... Done.
  <Sysname>
  ```

- Method 2:

  ```
  <Sysname> cd seclog
  <Sysname> undelete startup.cfg
  Undelete flash:/seclog/startup.cfg? [Y/N]:y
  Undeleting file flash:/seclog/startup.cfg... Done.
  ```

Contents

Configuration file management commands

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

archive configuration

Use **archive configuration** to manually archive the running configuration to the configuration archive directory.

Syntax

archive configuration

Views

User view

Predefined user roles

network-admin

Usage guidelines

This command saves the running configuration to the specified configuration archive directory with file names generated from the specified name prefix.

Before executing this command, you must use one of the following methods to specify a directory and a name prefix for the configuration archives:

- For local archiving, use the **archive configuration location** command to specify a local configuration archive directory and a name prefix.
- For remote archiving, use the **archive configuration server** command to specify a configuration archive directory and a name prefix on a remote SCP server. In addition, you must use the **archive configuration server user** and **archive configuration server password** commands to configure a username and password for accessing the server.

If you use the **archive configuration location** command to specify a local configuration archive directory, manual configuration archiving saves the running configuration only on the master device.

Examples

Archive the running configuration.

```
<Sysname> archive configuration
Save the running configuration to an archive file. Continue? [Y/N]: Y
The running configuration was saved to myarchive_1.cfg.
```

Related commands

archive configuration interval

archive configuration location

archive configuration max

archive configuration server

archive configuration server password

archive configuration server user

display archive configuration

archive configuration interval

Use **archive configuration interval** to enable automatic running-configuration archiving and set the archiving interval.

Use **undo archive configuration interval** to disable automatic running-configuration archiving.

Syntax

archive configuration interval *interval*

undo archive configuration interval

Default

The automatic running-configuration archiving feature is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the interval for automatically saving the running configuration. The value range is 10 to 525600, in minutes.

Usage guidelines

Automatic configuration archiving enables the system to periodically save the running configuration to the archive directory. After the system finishes an automatic archive, it resets the archiving interval timer.

Before enabling automatic configuration archiving, you must use one of the following methods to specify a directory and a name prefix for the configuration archives:

- For local archiving, use the **archive configuration location** command to specify a local configuration archive directory and a name prefix.
- For remote archiving, use the **archive configuration server** command to specify a configuration archive directory and a name prefix on a remote SCP server. In addition, you must use the **archive configuration server user** and **archive configuration server password** commands to configure a username and password for accessing the server.

If you use the **archive configuration location** command to specify a local configuration archive directory, automatic configuration archiving saves the running configuration only on the master device.

Examples

Set the system to archive the running configuration every 60 minutes.

```
<Sysname> system-view
[Sysname] archive configuration interval 60
Archive file will be saved every 60 minutes.
```

Related commands

archive configuration

archive configuration location

archive configuration max

archive configuration server

archive configuration server password

archive configuration server user

display archive configuration

archive configuration location

Use **archive configuration location** to specify a local directory and file name prefix for archiving the running configuration.

Use **undo archive configuration location** to restore the default.

Syntax

archive configuration location *directory* **filename-prefix** *filename-prefix*

undo archive configuration location

Default

No local directory or file name prefix is specified on the device for archiving the running configuration.

Views

System view

Predefined user roles

network-admin

Parameters

directory: Specifies the archive directory, a string of 1 to 63 characters. The value for this argument must take the format of *storage-medium-name:/folder-name*. The directory must already exist on the master.

filename-prefix: Specifies a file name prefix for configuration archives, a case-insensitive string of 1 to 30 characters. Valid characters are letters, digits, underscores (_), and hyphens (-).

Usage guidelines

Before archiving the running configuration, either manually or automatically, you must specify a local or remote directory and file name prefix for configuration archives.

The local configuration archives on the device are named in the format of *prefix_serial number***.cfg**, for example, **archive_1.cfg** and **archive_2.cfg**. The serial number is automatically assigned from 1 to 1000, increasing by 1. After the serial number reaches 1000, it restarts from 1.

If you change the file directory or file name prefix on the device, the following events occur:

- The old configuration archives change to common configuration files.
- The configuration archive counter is reset. The serial number for new configuration archives starts at 1.
- The **display archive configuration** command no longer displays the old configuration archives.

The configuration archive counter does not restart when you delete configuration archives from the archive directory. However, if the device reboots after all configuration archives have been deleted,

the configuration archive counter restarts. The serial number for new configuration archives starts at 1.

The **undo archive configuration location** command removes the local configuration archive directory and file name prefix settings. The command also performs the following operations:

- Disables the configuration archive feature (both manual and automatic methods).
- Restores the default settings of the **archive configuration interval** and **archive configuration max** commands.
- Clears the configuration archive information displayed by using the **display archive configuration** command.

Examples

Set the configuration archive directory as **flash:/archive** and the archive file name prefix as **my_archive**.

```
<Sysname> mkdir flash:/archive
Creating directory flash:/archive... Done.
<Sysname> system-view
[Sysname] archive configuration location flash:/archive filename-prefix my_archive
```

Related commands

archive configuration

archive configuration interval

archive configuration max

display archive configuration

archive configuration max

Use **archive configuration max** to set the maximum number of configuration archives that can be saved on the device.

Use **undo archive configuration max** to restore the default.

Syntax

archive configuration max *file-number*

undo archive configuration max

Default

The maximum number is 5.

Views

System view

Predefined user roles

network-admin

Parameters

file-number: Specifies the maximum number of configuration archives that can be saved on the device. The value range is 1 to 10. Adjust the setting depending on the amount of storage space available.

Usage guidelines

Before you execute this command, use the **archive configuration location** command to specify a configuration archive directory and archive file name prefix on the device.

After the maximum number of configuration archives is reached, the system deletes the oldest archive for the new archive.

Changing the limit setting to a lower value does not cause immediate deletion of excess archives. Instead, the configuration archive feature deletes the oldest *n* files when a new archive is manually or automatically saved, where *n* = current archive count – new archive limit + 1. For example, seven configuration archives have been saved before the archive limit is set to four. When saving a new configuration archive, the system first deletes the oldest four (7 – 4 + 1) archives.

If you execute the **undo archive configuration location** command, the default archive limit is restored.

Examples

Set the maximum number of configuration archives to 10.

```
<Sysname> system-view
[Sysname] archive configuration max 10
```

Related commands

archive configuration

archive configuration location

archive configuration interval

display archive configuration

archive configuration server

Use **archive configuration server** to configure the parameters for archiving the running configuration to a remote SCP server.

Use **undo archive configuration server** to restore the default.

Syntax

archive configuration server scp { *ipv4-address* | **ipv6** *ipv6-address* } [**port** *port-number*] [**directory** *directory*] **filename-prefix** *filename-prefix*

undo archive configuration server

Default

No parameters are set for archiving the running configuration to a remote SCP server.

Views

System view

Predefined user roles

network-admin

Parameters

scp: Specifies a remote SCP server.

ipv4-address: Specifies the SCP server by its IPv4 address.

ipv6 *ipv6-address*: Specifies the SCP server by its IPv6 address.

port *port-number*: Specifies the TCP port number of the SCP server. The value range for the *port-number* argument is 0 to 65535, and the default port number is 22.

directory *directory*: Specifies the archive directory, a case-insensitive string. If you do not specify this option, the archive directory is the root directory of the SCP server.

filename-prefix *filename-prefix*: Specifies a file name prefix for configuration archives, a case-insensitive string of 1 to 30 characters. Valid characters are letters, digits, underscores (_), and hyphens (-).

Usage guidelines

IMPORTANT:

In FIPS mode, the device does not support archiving the running configuration to a remote SCP server.

Before archiving the running configuration to a remote SCP server, you must perform the following tasks:

- Use this command to specify a configuration archive directory and a name prefix on the remote SCP server.
- Use the **archive configuration server user** and **archive configuration server password** commands to configure a username and password for accessing the server.

To manually archive the running configuration, use the **archive configuration** command. To periodically archive the running configuration, use the **archive configuration interval** command.

On the specified remote SCP server, configuration archives are named in the format of *filename-prefix_YYYYMMDD_HHMMSS***.cfg**, for example, **archive_20170526_203430.cfg**.

Local archiving (the **archive configuration location** command) and remote archiving (the **archive configuration server** command) are mutually exclusive. You cannot use the two features at the same time.

The maximum number of configuration archives on a remote SCP server depends on the SCP server setting and is not restricted by the **archive configuration max** command.

The **undo archive configuration server** command removes the configuration archive directory and file name prefix settings, but it does not delete the configuration archives saved on the server. The command also performs the following operations:

- Disables the configuration archive feature (both manual and automatic methods).
- Restores the default setting for the **archive configuration interval** command.
- Clears the configuration archive information displayed by using the **display archive configuration** command.

Examples

Set the configuration archive directory as **archive/** on the SCP server at 192.168.1.1 and set the archive file name prefix as **my_archive**.

```
<Sysname> system-view
[Sysname] archive configuration server scp 192.168.1.1 port 22 directory /archive/
filename-prefix my_archive
```

Related commands

archive configuration

archive configuration interval

archive configuration location

archive configuration server password

archive configuration server user

display archive configuration

archive configuration server password

Use **archive configuration server password** to configure the password for accessing the SCP server that saves the configuration archives.

Use **undo archive configuration server password** to restore the default.

Syntax

archive configuration server password { **cipher** | **simple** } *string*

undo archive configuration server password

Default

No password is configured for accessing the SCP server that saves the configuration archives.

Views

System view

Predefined user roles

network-admin

Parameters

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 63 characters. Its encrypted form is a case-sensitive string of 33 to 117 characters.

Examples

Set the password to **admin** in plaintext form for accessing the SCP server that saves the configuration archives.

```
<Sysname> system-view
[Sysname] archive configuration server password simple admin
```

Related commands

archive configuration server

archive configuration server user

display archive configuration

archive configuration server user

Use **archive configuration server user** to configure the username for accessing the SCP server that saves the configuration archives.

Use **undo archive configuration server user** to restore the default.

Syntax

archive configuration server user *user-name*

undo archive configuration server user

Default

No username is configured for accessing the SCP server that saves the configuration archives.

Views

System view

Predefined user roles

network-admin

Parameters

user-name: Specifies the username, a case-sensitive string of 1 to 63 characters.

Examples

Set the username to **admin** for accessing the SCP server that saves the configuration archives.

```
<Sysname> system-view
[Sysname] archive configuration server user admin
```

Related commands

archive configuration server

archive configuration server password

display archive configuration

backup startup-configuration

Use **backup startup-configuration** to back up the main next-startup configuration file to a TFTP server.

Syntax

backup startup-configuration to { *ipv4-server* | **ipv6** *ipv6-server* } [*dest-filename*]

Views

User view

Predefined user roles

network-admin

Parameters

ipv4-server: Specifies a TFTP server by its IPv4 address or host name. The host name is a case-insensitive string of 1 to 253 characters. Valid characters include letters, digits, hyphens (-), underscores (_), and dots (.).

ipv6 *ipv6-server*: Specifies a TFTP server by its IPv6 address or host name. The host name is a case-insensitive string of 1 to 253 characters. Valid characters include letters, digits, hyphens (-), underscores (_), and dots (.).

dest-filename: Specifies the name of the target file used for saving the file on the server. The file must be a .cfg file. The file name is a case-insensitive string of up to 255 characters. If you do not specify a target file name, the source file name is used.

Usage guidelines

This command is not supported in FIPS mode.

Examples

Back up the main next-startup configuration file to the IPv4 TFTP server at 2.2.2.2, and set the target file name to **192-168-1-26.cfg**.

```
<Sysname> backup startup-configuration to 2.2.2.2 192-168-1-26.cfg
Backing up the main startup configuration file to 2.2.2.2...
```

```
Done.
```

Back up the main next-startup configuration file to the IPv6 TFTP server at 2001::2, and set the target file name to **192-168-1-26.cfg**.

```
<Sysname> backup startup-configuration to ipv6 2001::2 192-168-1-26.cfg
Backing up the main startup configuration file to 2001::2...
Done.
```

Related commands

`restore startup-configuration`

configuration commit

Use **`configuration commit`** to commit the settings configured after the configuration commit delay timer was set.

Syntax

`configuration commit`

Views

System view

Predefined user roles

network-admin

Usage guidelines

You must execute the **`configuration commit delay`** command to set the configuration delay timer before executing this command.

The settings you made during the commit delay interval are automatically removed if you have not manually committed them before the configuration commit delay timer expires.

As a best practice, configure the information center to output logs to the console. Use the logs to determine whether you want to commit the settings. For more information about the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Set the configuration commit delay timer to 10 minutes.

```
<Sysname> system-view
[Sysname] configuration commit delay 10
```

Commit the settings configured after the configuration commit delay timer was set and before the delay timer expires.

```
[Sysname] configuration commit
```

Related commands

`configuration commit delay`

configuration commit delay

Use **`configuration commit delay`** to enable the configuration commit delay feature and start the configuration commit delay timer.

Syntax

`configuration commit delay` *`delay-time`*

Views

System view

Predefined user roles

network-admin

Parameters

delay-time: Sets the configuration commit delay interval. The value range is 1 to 65535 minutes.

Usage guidelines

The system creates a rollback point to record the configuration status when you execute this command to start the configuration commit delay timer. The settings you made during the commit delay interval takes effect immediately. However, these settings will be removed automatically if you have not manually committed them before the configuration commit delay timer expires. Then, the system returns to the configuration status when the commit delay timer started.

This feature prevents a misconfiguration from causing the inability to access the device and is especially useful when you configure the device remotely.

When you use this feature, follow these restrictions and guidelines:

- In a multi-user context, make sure no one else is configuring the device.
- To avoid unexpected errors, do not perform any operations during the configuration rollback.
- You can reconfigure the configuration commit delay timer before it expires to shorten or extend the commit delay interval. However, the rollback point will not change.
- The configuration commit delay feature is a one-time setting. The feature is disabled with the rollback point removed when the commit delay timer expires or after a manual commit operation is performed. To use this feature again, you must re-execute this command.

Examples

Set the configuration commit delay timer to 10 minutes.

```
<Sysname> system-view
[Sysname] configuration commit delay 10
```

Change the configuration commit delay timer to 60 minutes before the old delay timer expires.

```
[Sysname] configuration commit delay 60
The commit delay already set 10 minutes, overwrite it? [Y/N]:y
```

Related commands

configuration commit

configuration encrypt

Use **configuration encrypt** to enable configuration encryption.

Use **undo configuration encrypt** to disable configuration encryption.

Syntax

configuration encrypt { **private-key** | **public-key** }

undo configuration encrypt

Default

Configuration encryption is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

`private-key`: Encrypts configuration with a private key. All devices running Comware 7 software use the same private key.

`public-key`: Encrypts configuration with a public key. All devices running Comware 7 software use the same public key.

Usage guidelines

Configuration encryption enables the device to automatically encrypt a configuration file when saving the running configuration to the file.

Any devices running Comware 7 software can decrypt the encrypted configuration file. To prevent an encrypted file from being decoded by unauthorized users, make sure the file is accessible only to authorized users.

Examples

Enable the public-key method for configuration encryption.

```
<Sysname> system-view
[Sysname] configuration encrypt public-key
```

configuration replace file

Use **`configuration replace file`** to perform configuration rollback.

Syntax

`configuration replace file` *`filename`*

Views

System view

Predefined user roles

network-admin

Parameters

`filename`: Specifies the path of the replacement configuration file, a string of up to 255 characters. The file must be a .cfg file. The file and file path must be valid and on the local system.

Usage guidelines

CAUTION:

The configuration rollback feature replaces the running configuration with the configuration in a configuration file without rebooting the device. This operation will cause settings not in the replacement configuration file to be lost, which might cause service interruption. When you perform configuration rollback, make sure you fully understand its impact on your network.

The configuration rollback feature helps you revert to a previous configuration state or adapt the running configuration to different network environments.

To ensure a successful rollback, follow these guidelines:

- Make sure the replacement configuration file is created by using the configuration archive feature or the **`save`** command on the device.
- If the configuration file is not created on the device, make sure the command lines in the configuration file are fully compatible with the device.

- If the replacement configuration file is encrypted, make sure the device can decrypt it.

Examples

Replace the running configuration with the configuration in the **my_archive_1.cfg** configuration file.

```
<Sysname> system-view
[Sysname] configuration replace file my_archive_1.cfg
Current configuration will be lost, save current configuration? [Y/N]:n
Now replacing the current configuration. Please wait...
Succeeded in replacing current configuration with the file my_archive_1.cfg.
```

display archive configuration

Use **display archive configuration** to display configuration archive information.

Syntax

display archive configuration

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display information about the configuration archives. The sample output was created based on local archiving.

```
<Sysname> display archive configuration
Location: flash:/archive
Filename prefix: my_archive
Archive interval in minutes: 120
Maximum number of archive files: 10
Archive history:
  No.  Timestamp               Filename
  1    Aug 05 2007 20:24:54    my_archive_1.cfg
  2    Aug 05 2007 20:34:54    my_archive_2.cfg
# 3    Aug 05 2007 20:44:54    my_archive_3.cfg
The pound sign (#) indicates the most recent archive file.
Next archive file to be saved: my_archive_4.cfg
```

Display information about the configuration archives. The sample output was created based on remote archiving.

```
<Sysname> display archive configuration
Username: test
Location: scp://192.168.21.21:22/archive
Filename prefix: my_archive
Archive interval in minutes: 120
Archive history:
 No.   Timestamp                  Filename
 1    Wed Dec 15 14:20:18 2010   my_archive_20170509_142018.cfg
!2    Wed Dec 15 14:33:10 2010   my_archive_20170509_143018.cfg
```

```
#!3    Wed Dec 15 14:49:37 2010   my_archive_20170509_144018.cfg
The exclamation mark (!) indicates that the remote archiving attempt failed.
The pound sign (#) indicates the most recent archive file.
```

Table 1 Command output

Field	Description
Username	Username for accessing the SCP server that saves the configuration archives.
Location	Absolute path of the directory for saving running-configuration archives.
Filename prefix	File name prefix for configuration archives.
Archive interval in minutes	Interval (in minutes) for the system to automatically archive the running configuration. If automatic configuration saving is disabled, this field is not available.
Maximum number of archive files	Maximum number of configuration archives that can be saved on the device.
Archive history	History configuration archive information.
No.	Number of a configuration archive.
Timestamp	Time when the configuration archive was created.

Related commands

archive configuration

archive configuration interval

archive configuration location

archive configuration max

archive configuration server

archive configuration server user

display current-configuration

Use **display current-configuration** to display the running configuration.

Syntax

display current-configuration [[**configuration** [*module-name*] | **interface** [*interface-type* [*interface-number*]]] [**all**] | **slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

configuration [*module-name*]: Displays the feature configuration. The *module-name* argument specifies a feature module. If you do not specify a feature module, the command displays all feature settings you have made.

interface [*interface-type* [*interface-number*]]: Displays interface configuration, where the *interface-type* argument represents the interface type and the *interface-number* argument represents the interface number. If you do not specify the *interface-type interface-number* arguments, the command displays the running configuration for all interfaces. If you specify only the *interface-type* argument, the command displays the running configuration for all interfaces of this type.

all: Displays all settings in the running configuration, including the default settings. If you do not specify this keyword, the command displays only non-default settings in the running configuration.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify an IRF member device, this command displays the running configuration for all IRF member devices.

NOTE:

The **all** keyword is supported only in Release 6343P08 and later.

Usage guidelines

Use this command to verify the configuration you have made.

If the system has automatically changed the setting you have made for a parameter, this command displays the effective setting instead of the configured one. An automatic change typically occurs because of system restrictions. This command does not display parameters that are using the default settings.

Examples

Display local user configuration.

```
<Sysname> display current-configuration configuration local-user
#
local-user ftp
 password hash
$h$6$Twd73mLrN8O2vvD5$Cz1vgdpR4KoTiRQNE9pg33gU14Br2p1VguczLSVyJLO2huV5Syx/LfDIf8ROLtV
ErJ/C31oq2rFtmNuyZf4STw==
 service-type ftp
 authorization-attribute user-role network-operator
#
local-user root
 password hash
$h$6$Twd73mLrN8O2vvD5$Cz1vgdpR4KoTiRQNE9pg33gU14Br2p1VguczLSVyJLO2huV5Syx/LfDIf8ROLtV
ErJ/C31oq2rFtmNuyZf4STw==
 service-type ssh telnet terminal
 authorization-attribute user-role network-admin
#
return
```

Display VLAN interface configuration.

```
<Sysname> display current-configuration interface Vlan-interface
#
interface Vlan-interface1
 ip address 192.168.1.84 255.255.255
#
Return
```

display current-configuration diff

Use **display current-configuration diff** to display the differences that the running configuration has as compared with the next-startup configuration.

Syntax

display current-configuration diff

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

This command searches for the next-startup configuration in the following order:

1. The .cfg main next-startup configuration file.
2. The .cfg backup next-startup configuration file if the .cfg main next-startup configuration file is unavailable.

If both configuration files are unavailable, the system displays a message indicating that no next-startup configuration files exist.

Examples

Display the differences that the running configuration has as compared with the next-startup configuration.

```
<Sysname> display current-configuration diff
--- Startup configuration
+++ Current configuration
@@ -5,7 +5,7 @@
 #
  sysname Sysname
 #
-alias dhc display history-command
+alias dh display hotkey
 #
  system-working-mode standard
<Sysname>
```

Table 2 Command output

Field	Description
--- *A* +++ *B*	• *A* represents the source configuration for comparison, which can be **Startup configuration**, **Current configuration**, or the name of the source configuration file with its directory information. • *B* represents the target configuration for comparison, which can be **Current configuration**, **Startup configuration**, or the name of the target configuration file with its directory information. In this example, the startup configuration and the current configuration are the source and target, respectively.

Field	Description
@@ -linenumber1,number1 +linenumber2,number2 @@	Location information for identifying the command line differences: • *-linenumber1,number1*—Source configuration section that contains differences. The *linenumber1* argument represents the start line of the section. The *number1* argument represents the number of lines between the start line and the end line of the section. • *+linenumber2,number2*—Target configuration section that contains differences. The *linenumber2* argument represents the start line of the section. The *number2* argument represents the number of lines between the start line and the end line of the section.
cmd1 *- cmd2* *+ cmd3* *cmd4*	Displays command differences. • *cmd1* and *cmd4*—Command lines are contained in both source and target configurations if they are not prefixed with a minus (-) or plus (+) sign. They provide a context for locating command line differences. • *- cmd2*—Command lines are prefixed with a minus sign if they are contained in the source configuration but not in the target configuration. • *+ cmd3*—Command lines are prefixed with a plus sign if they are contained in the target configuration but not in the source configuration. In this example, the sample output shows that the **`alias dhc display history-command`** command is contained only in the source configuration, and the **`alias dh display hotkey`** command is contained only in the target configuration.

Related commands

`display current-configuration`

`display diff`

`display saved-configuration`

display default-configuration

Use **`display default-configuration`** to display the factory defaults.

Syntax

`display default-configuration`

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

Factory defaults are custom basic settings that came with the device. Factory defaults vary by device models and might differ from the initial default settings for the commands.

The device starts up with the factory defaults if no next-startup configuration files are available.

Examples

Display the factory defaults.

```
<Sysname> display default-configuration
```

display diff

Use **display diff** to display differences between configurations.

Syntax

display diff configfile *file-name-s* { **configfile** *file-name-d* | **current-configuration** | **startup-configuration** }

display diff current-configuration { **configfile** *file-name-d* | **startup-configuration** }

display diff startup-configuration { **configfile** *file-name-d* | **current-configuration** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

configfile *file-name-s*: Specifies the source configuration file for comparison.

configfile *file-name-d*: Specifies the target configuration file for comparison.

current-configuration: Specifies the running configuration. In the **display diff current-configuration** command, this keyword specifies the source configuration for comparison. In the **display diff configfile** *file-name-s* and **display diff startup-configuration** commands, this keyword specifies the target configuration.

startup-configuration: Specifies the next-startup configuration. In the **display diff startup-configuration** command, this keyword specifies the source configuration for comparison. In the **display diff configfile** *file-name-s* and **display diff current-configuration** commands, this keyword specifies the target configuration.

Usage guidelines

If you specify the **startup-configuration** keyword, the system searches for the next-startup configuration in the following order:

1. The .cfg main next-startup configuration file.
2. The .cfg backup next-startup configuration file if the .cfg main next-startup configuration file is unavailable.

If both configuration files are unavailable, the system displays a message indicating that no next-startup configuration files exist.

Examples

Display the differences between **startup.cfg** and **test.cfg**.

```
<Sysname> display diff configfile startup.cfg configfile test.cfg
--- flash:/startup.cfg
+++ flash:/test.cfg
@@ -5,7 +5,7 @@
 #
  sysname Sysname
 #
-alias dhc display history-command
```

```
+alias dh display hotkey
 #
  system-working-mode standard
<Sysname>
```

The output shows that the **alias dhc display history-command** command is contained only in **startup.cfg**, and the **alias dh display hotkey** command is contained only in **test.cfg**.

Display the differences between the running configuration and the next-startup configuration.

```
<Sysname> display diff current-configuration startup-configuration
--- Current configuration
+++ Startup configuration
@@ -5,7 +5,7 @@
 #
  sysname Sysname
 #
-alias dhc display history-command
+alias dh display hotkey
 #
  system-working-mode standard
<Sysname>
```

The output shows that the **alias dhc display history-command** command is contained only in the running configuration, and the **alias dh display hotkey** command is contained only in the next-startup configuration.

For the command output description, see Table 2.

Related commands

display current-configuration

display current-configuration diff

display saved-configuration

display saved-configuration

Use **display saved-configuration** to display the contents of the configuration file for the next system startup.

Syntax

display saved-configuration

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

Use this command to verify that important settings have been saved to the configuration file for the next system startup.

This command selects the configuration file to display in the following order:

1. If the main startup configuration file is available, this command displays the contents of the main startup configuration file.
2. If only the backup startup configuration file is available, this command displays the contents of the backup file.
3. If both the main and backup startup configuration files are not available, this command does not display anything.

Examples

Display the contents of the configuration file for the next system startup.

```
<Sysname> display saved-configuration
#
 version 7.1.070, Release 1201
#
 sysname Sysname
#
 ftp server enable
#
 telnet server enable
#
 domain default enable system
#
vlan 1
#
domain system
#
  ---- More ----
```

Related commands

reset saved-configuration

save

display startup

Use **display startup** to display the names of the current startup configuration file and the next-startup configuration files.

Syntax

display startup

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

All IRF members use the same current startup configuration file as the master.

After a master/subordinate switchover, it is normal that the current startup configuration files on all IRF members are displayed as NULL. This is because the new master continues to run with the running configuration rather than rebooting with a startup configuration file.

Examples

Display names of the startup configuration files.

```
<Sysname> display startup
MainBoard:
 Current startup saved-configuration file: flash:/startup.cfg(*)
 Next main startup saved-configuration file: flash:/startup.cfg
 Next backup startup saved-configuration file: NULL
```

Table 3 Command output

Field	Description
MainBoard	Displays the startup configuration files on the master device.
Current startup saved-configuration file	Configuration file that the device has started up with. If the field is suffixed with an asterisk (*), the startup configuration file is a binary configuration file.
Next main startup saved-configuration file	Primary configuration file to be used at the next startup.
Next backup startup saved-configuration file	Backup configuration file to be used at the next startup.

Related commands

`startup saved-configuration`

display this

Use **`display this`** to display the running configuration in the current view.

Syntax

`display this [ all ]`

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

`all`: Displays all settings in the running configuration in the current view, including the default settings. If you do not specify this keyword, the command displays only non-default settings in the running configuration.

NOTE:

The **`all`** keyword is supported only in Release 6343P08 and later.

Usage guidelines

Use this command to verify the configuration you have made in a certain view.

This command does not display parameters that are using the default settings.

Some parameters can be successfully set even if their dependent features are not enabled. For these parameters, this command displays their settings after the dependent features are enabled.

This command can be executed in any user line view to display the running configuration of all user lines.

Examples

Display the running configuration on VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] display this
#
interface Vlan-interface1
#
return
```

reset saved-configuration

Use **reset saved-configuration** to delete a next-startup configuration file.

Syntax

reset saved-configuration [**backup** | **main**]

Views

User view

Predefined user roles

network-admin

Parameters

backup: Specifies the backup next-startup configuration file.

main: Specifies the main next-startup configuration file.

Usage guidelines

CAUTION:

By default, this command permanently deletes the specified next-startup configuration file from all IRF member devices. To delete the configuration file only from the master device, disable automatic system-wide next-startup configuration file operations. For more information about disabling these operations, see *Fundamentals Configuration Guide*.

You can delete the main file, the backup file, or both.

To delete a file that is set as both main and backup next-startup configuration files, you must execute both the **reset saved-configuration backup** command and the **reset saved-configuration main** command. Using only one of the commands sets the target file attribute to NULL instead of deleting the file.

If you do not specify a configuration file attribute, the **reset saved-configuration** command deletes the main next-startup configuration file.

Examples

Delete the main next-startup configuration file.

```
<Sysname> reset saved-configuration
The saved configuration file will be erased. Are you sure? [Y/N]:y
Configuration file in flash: is being cleared.
Please wait ...........
Configuration file is cleared.
```

Related commands

display saved-configuration

restore startup-configuration

Use **restore startup-configuration** to download a configuration file from a TFTP server and specify it as the main next-startup configuration file.

Syntax

restore startup-configuration from { *ipv4-server* | **ipv6** *ipv6-server* } *src-filename*

Views

User view

Predefined user roles

network-admin

Parameters

ipv4-server: Specifies a TFTP server by its IPv4 address or host name. The host name is a case-insensitive string of 1 to 253 characters. Valid characters include letters, digits, hyphens (-), underscores (_), and dots (.).

ipv6 *ipv6-server*: Specifies a TFTP server by its IPv6 address or host name. The host name is a case-insensitive string of 1 to 253 characters. Valid characters include letters, digits, hyphens (-), underscores (_), and dots (.).

src-filename: Specifies the name of the configuration file to be downloaded. The file must be a .cfg file. The file name is a case-insensitive string of up to 255 characters.

Usage guidelines

This command is not supported in FIPS mode.

Before restoring the configuration file for the next startup, make sure the following requirements are met:

- The server is reachable.
- The server is enabled with TFTP service.
- You have read and write permissions to the server.

This command downloads the configuration file to the root directory of the default storage medium on each member device and specifies the file as the main next-startup configuration file. If a partitioned USB disk is used as the default storage medium, the configuration file is saved on the first partition. Make sure all IRF members use the same type of default storage media. If a subordinate device uses a different type of default storage medium than the master, the command cannot propagate the configuration file to the subordinate device. For example, the subordinate device uses a USB disk, but the master uses a flash memory. In this situation, you must manually restore the main next-startup configuration file on the subordinate device.

Examples

Download **test.cfg** from the IPv4 TFTP server at 2.2.2.2, and specify the file as the main next-startup configuration file.

```
<Sysname> restore startup-configuration from 2.2.2.2 test.cfg
Restoring the next startup-configuration file from 2.2.2.2. Please wait...finished.
```

Download **test.cfg** from the IPv6 TFTP server at 2001::2, and specify the file as the main next-startup configuration file.

```
<Sysname> restore startup-configuration from ipv6 2001::2 test.cfg
```

```
Restoring the next startup-configuration file from 2001::2. Please wait...finished.
```

Related commands

backup startup-configuration

save

Use **save** *file-url* [**all** | **slot** *slot-number*] to save the running configuration to a configuration file, without specifying the file as a next-startup configuration file.

Use **save** [**safely**] [**backup** | **main**] [**force**] [**changed**] to save the running configuration as a next-startup configuration file in the root directory of the storage medium.

Syntax

save *file-url* [**all** | **slot** *slot-number*]

save [**safely**] [**backup** | **main**] [**force**] [**changed**]

Views

Any view

Predefined user roles

network-admin

Parameters

file-url: Specifies a file path, a string of up to 255 characters. The file must be a .cfg file. If you specify the **all** keyword or the **slot** *slot-number* option, the file path cannot include a member ID. If the file path includes a folder name, the folder must already exist on the specified IRF member devices.

all: Saves the running configuration to all member devices. If you do not specify this keyword or the **slot** *slot-number* option, the command saves the running configuration only to the master.

slot *slot-number*: Specifies a subordinate device by its member ID. If you do not specify a subordinate device or the **all** keyword, this command saves the running configuration only to the master.

safely: Saves the configuration file in safe mode. If you do not specify this keyword, the device saves the configuration file in fast mode.

backup: Saves the running configuration to a configuration file, and specifies the file as the backup next-startup configuration file. If you do not specify this keyword or the **main** keyword, the command specifies the saved file as the main next-startup configuration file.

main: Saves the running configuration to a configuration file, and specifies the file as the main next-startup configuration file. If you do not specify this keyword or the **backup** keyword, the command specifies the saved file as the main next-startup configuration file.

force: Saves the running configuration to the existing next-startup configuration file without prompting for confirmation. If you do not specify this keyword, the system prompts you to confirm the operation. If you do not confirm the operation within 30 seconds, the system automatically aborts the operation. If you enter **Y** within the time limit, you can continue the save process and change the target file name during the process.

changed: Overwrites the target configuration file with the running configuration if an inconsistency is detected between the settings in the configuration file and the running configuration. The **save** command does not take effect if no inconsistency is detected. If you do not specify this keyword, the **save** command always overwrites the target configuration file with the running configuration.

Usage guidelines

CAUTION:

Use the **save** command with caution. This command will overwrite the settings in the target configuration file. When you execute this command, carefully read the messages displayed by the system and make sure you fully understand the impact of this command on services.

If the file specified for this command does not exist, the system creates the file before saving the configuration. If the file already exists, the system prompts you to confirm whether to overwrite the file. If you choose to not overwrite the file, the system cancels the save operation.

This command saves the running configuration to an .mdb binary file as well as a .cfg text file. The two files use the same file name. An .mdb file takes less time to load than a .cfg file.

When you use the **save** [**safely**] [**backup** | **main**] [**force**] [**changed**] command, follow these guidelines:

- In safe mode, the system saves configuration in a temporary file and starts overwriting the target next-startup configuration file after the save operation is complete. If a reboot, power failure, or out of memory or storage space event occurs during the save operation, the next-startup configuration file is retained.
- In fast mode, the device directly overwrites the target next-startup configuration file. If a reboot, power failure, or out of memory or storage space event occurs during this process, all settings in the next-startup configuration file are lost.

Safe mode is slower than fast mode, but more secure. As a best practice, specify the **safely** keyword for reliable configuration saving.

By default, the **save** [**safely**] [**backup** | **main**] [**force**] [**changed**] command saves the configuration to all IRF member devices. To save the configuration only to the master device, disable automatic system-wide next-startup configuration file operations. For more information about disabling these operations, see *Fundamentals Configuration Guide*.

Examples

Save the running configuration to **backup.cfg**, without specifying the file as a next-startup configuration file.

```
<Sysname> save backup.cfg
The current configuration will be saved to flash:/backup.cfg. Continue? [Y/N]:y
Now saving current configuration to the device.
Saving configuration flash:/backup.cfg. Please wait...
Configuration is saved to device successfully.
```

Save the running configuration to the main next-startup configuration file without any confirmation required.

```
<Sysname> save force
Validating file. Please wait....
Saved the current configuration to mainboard device successfully.
```

Save the running configuration to a file in the root directory of the default storage medium, and specify the file as the main next-startup configuration file.

```
<Sysname> save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/backup.cfg]
(To leave the existing filename unchanged, press the enter key):test.cfg
Validating file. Please wait.....
Saved the current configuration to mainboard device successfully.
```

Related commands

display current-configuration

display saved-configuration

standby auto-update config

Use **standby auto-update config** to enable automatic system-wide next-startup configuration file operations.

Use **undo standby auto-update config** to disable automatic system-wide next-startup configuration file operations.

Syntax

standby auto-update config

undo standby auto-update config

Default

Next-startup configuration file operations are automatically synchronized across the entire system.

Views

System view

Predefined user roles

network-admin

Usage guidelines

By default, automatic system-wide next-startup configuration file operations are enabled. The system performs the following operations on all IRF subordinate devices in addition to the master device:

- Saves the running configuration to the next-startup configuration file on each member device when you execute the **save** [**safely**] [**backup** | **main**] [**force**] [**changed**] command.
- Deletes the next-startup configuration file on each member device when you execute the **reset saved-configuration** command.

If you disable automatic system-wide next-startup configuration file operations, the system saves the running configuration or deletes the next-startup configuration file only on the master device.

Automatic system-wide operations ensure start-up configuration file consistency between the master and subordinate devices. However, a system-wide operation takes more time than an operation performed only on the master device. In addition, the amount of time required to complete a system-wide configuration operation increases as the amount of configuration data grows.

If you are disabling automatic system-wide operations for faster configuration saving, be aware that the next-startup configuration files will be inconsistent between the master device and the subordinate devices.

Examples

Enable automatic system-wide next-startup configuration file operations.

```
<Sysname> system-view
[Sysname] standby auto-update config
```

Related commands

reset saved-configuration

save

startup saved-configuration

Use **startup saved-configuration** to specify a file as a next-startup configuration file.

Use **undo startup saved-configuration** to configure the system to start up with the factory defaults at the next startup.

Syntax

startup saved-configuration *cfgfile* [**backup** | **main**]

undo startup saved-configuration

Default

No next-startup configuration files are specified.

Views

User view

Predefined user roles

network-admin

Parameters

cfgfile: Specifies the path of a configuration file, a string of up to 255 characters. The file must be a .cfg file. The file path can include only the file name, or the storage medium information and file name. If the file is not on the default storage medium, you must specify the file name with storage medium information.

backup: Specifies the configuration file as the backup next-startup configuration file.

main: Specifies the configuration file as the main next-startup configuration file. This is the primary configuration file that the device attempts to load at startup. If the loading attempt fails, the device tries the backup next-startup configuration file.

Usage guidelines

CAUTION:

In an IRF fabric, the **undo startup saved-configuration** command can cause an IRF split after the IRF fabric or an IRF member reboots.

The **startup saved-configuration** command applies to all IRF members. To successfully execute this command, make sure the specified file has been saved in the root directory of the storage medium on each member.

If you do not specify the **backup** or **main** keyword, the **startup saved-configuration** command specifies the main next-startup configuration file.

As a best practice, specify different files as the main and backup next-startup configuration files.

The **undo startup saved-configuration** command changes the file attribute of the main and backup next-startup configuration files to NULL. However, the command does not delete the two configuration files.

You can also specify a configuration file as a next startup file when you use the **save** command to save the running configuration.

Examples

Specify the main next-startup configuration file.

```
<Sysname> startup saved-configuration testcfg.cfg
Please wait ....... Done.
```

Related commands

display startup

Contents

Software upgrade commands

As a best practice, store the startup images in a fixed storage medium. If you store the startup images in a hot swappable storage medium, do not remove the hot swappable storage medium during the startup process.

boot-loader file

Use **boot-loader file** to specify startup image files.

Syntax

boot-loader file boot *filename* **system** *filename* [**feature** *filename*&<1-30>] [**patch** *filename*&<1-16>] { **all** | **slot** *slot-number* } { **backup** | **main** }

boot-loader file *ipe-filename* [**patch** *filename*&<1-16>] { **all** | **slot** *slot-number* } { **backup** | **main** }

Views

User view

Predefined user roles

network-admin

Parameters

boot: Specifies a boot image file.

system: Specifies a system image file.

feature: Specifies a space-separated list of up to 30 feature image files.

patch: Specifies a space-separated list of up to 16 patch image files. You can specify only non-incremental patch image files.

filename: Specifies a .bin file in the *filesystemname*:*filename***.bin** format. The file must be stored in the root directory of a file system on the device. Excluding the file system location section (if any), the value string can have a maximum of 63 characters. For more information about specifying a file, see *Fundamentals Configuration Guide*.

ipe-filename: Specifies an .ipe image package file in the *filesystemname*:*filename***.ipe** format. The file must be stored in the root directory of a file system on the device. Excluding the file system location section (if any), the value string can have a maximum of 63 characters. For more information about specifying a file, see *Fundamentals Configuration Guide*.

all: Specifies all hardware components to which the specified images apply.

slot *slot-number*: Specifies the IRF member ID of a member device.

backup: Specifies the files as backup startup image files. Backup images are used only when main images are not available.

main: Specifies the files as main startup image files. The device always first attempts to start up with main startup files.

Usage guidelines

The **boot-loader file** command overwrites the entire startup image list. To add new startup feature images, specify all feature image files in the old startup image list, including feature image files. The new startup image list will contain only the feature image files that are specified in the command.

To load the specified startup software images, you must reboot the system.

If the upgrade images are not found in the file system on the slot specified to upgrade, the system automatically copies the images to that file system. The destination directory is the root directory of the file system. If the destination root directory already contains a startup image with the same name as an upgrade image, you must choose whether to overwrite the image.

Examples

Specify **flash:/all.ipe** as the main startup image file for slot 1.

```
<Sysname> boot-loader file flash:/all.ipe slot 1 main
Verifying the IPE file and the images.....Done.
H3C S5130S-28S-HPWR-LI Switch images in IPE:
  boot.bin
  system.bin
  feature.bin
This command will set the main startup software images. Continue? [Y/N]:Y
Add images to slot 1.
File flash:/boot.bin already exists on slot 1.
File flash:/system.bin already exists on slot 1.
File flash:/feature.bin already exists on slot 1.
Overwrite the existing files? [Y/N]:Y
Decompressing file boot.bin to flash:/boot.bin.....Done.
Decompressing file system.bin to flash:/system.bin.....Done.
Decompressing file feature.bin to flash:/feature.bin.....Done.
Verifying the file flash:/boot.bin on slot 1...Done.
Verifying the file flash:/system.bin on slot 1.....Done.
Verifying the file flash:/feature.bin on slot 1.....Done.
The images that have passed all examinations will be used as the main startup software
images at the next reboot on slot 1.
```

Specify **flash:/all.ipe** as the main startup image file for all IRF member devices.

```
<Sysname> boot-loader file slot1#flash:/all.ipe all main
Verifying the file flash:/all.ipe on slot 1.....Done.
H3C S5130S-28S-HPWR-LI Switch images in IPE:
  boot.bin
  system.bin
  feature.bin
This command will set the main startup software images. Continue? [Y/N]:y
Add images to slot 1.
File flash:/boot.bin already exists on slot 1.
File flash:/system.bin already exists on slot 1.
File flash:/feature.bin already exists on slot 1.
Overwrite the existing files? [Y/N]:y
Decompressing file boot.bin to flash:/boot.bin.....Done.
Decompressing file system.bin to flash:/system.bin.....Done.
Decompressing file feature.bin to flash:/feature.bin.....Done.
The images that have passed all examinations will be used as the main startup software
images at the next reboot on slot 1.
File flash:/boot.bin already exists on slot 2.
Do you want to overwrite the file?
 Y: Overwrite the file.
```

```
 N: Not overwrite the file.
 A: From now on, overwrite or not overwrite without prompt.
Please make a choice. [Y/N/A]:a
What type of overwrite operation do you want to perform?
 Y: Overwrite without prompt.
 N: Not overwrite or display prompt.
 Q: Return to the previous step.
Please make a choice. [Y/N/Q]:y
An existing file will be overwritten without prompt if it has the same name as any upgrade
file.
Loading.....................Done.
Loading.....................Done.
Loading.....................Done.
Loading.....................Done.
Loading.....................Done.
Loading.....................Done.
Loading.....................Done.
Loading.....................Done.
Loading.....................Done.
The images that have passed all examinations will be used as the main startup software
images at the next reboot on slot 2.
The images that have passed all examinations will be used as the main startup software
images at the next reboot on slot 3.
Decompression completed.
Do you want to delete flash:/all.ipe now? [Y/N]:n
```

Related commands

display boot-loader

boot-loader update

Use **boot-loader update** to synchronize startup images.

Syntax

boot-loader update { **all** | **slot** *slot-number* }

Views

User view

Predefined user roles

network-admin

Parameters

all: Synchronizes startup images from the master to all subordinate devices.

slot *slot-number*: Specifies the IRF member ID of a subordinate device.

Usage guidelines

You can use this command to synchronize startup images after adding new member devices.

The startup images synchronized to the subordinate device are set as main startup images, regardless of whether the source startup images are main or backup.

- If the master device has started up with main startup images, its main startup images are synchronized to the subordinate device, regardless of whether any main startup image has been respecified on the master device.
- If the master device has started up with backup startup images, its backup startup images are synchronized to the subordinate device, regardless of whether any backup startup image has been respecified on the master device.

If patches have been installed on the master, use the **install commit** command to update the set of main startup images on the master before software synchronization. This command ensures startup image consistency between the master and the subordinate device.

Startup image synchronization fails if any software image being synchronized is not available or is corrupted.

Examples

Synchronize startup images to a slot.

```
<Sysname> boot-loader update slot 2
This command will update the specified standby MPU. Continue? [Y/N]:y
Updating. Please wait...
Verifying the file flash:/s5130s_li-cmw710-boot-a6103p06.bin on slot 1...Done.
Verifying the file flash:/s5130s_li-cmw710-system-a6103p06.bin on slot 1....Done.
Verifying the file flash:/s5130s_li -cmw710-devkit-a6103p06.bin on slot 1...Done.
Copying main startup software images to slot 2. Please wait...
Done.
Setting copied images as main startup software images for slot 2...
The images that have passed all examinations will be used as the main startup software
images at the next reboot on slot 2.
Done.
Successfully updated the startup software images of slot 2.
```

Related commands

display boot-loader

bootrom update

Use **bootrom update** to load the BootWare image from a file system to the Normal BootWare area.

Syntax

bootrom update file *file* **slot** *slot-number-list*

Views

User view

Predefined user roles

network-admin

Parameters

file *file*: Specifies the file that contains the BootWare image. The *file* argument represents the file name, a string of 1 to 63 characters.

slot *slot-number-list*: Specifies a space-separated list of up to seven slot number items. An item specifies an IRF member device by its member ID or a range of IRF member devices in the form of *start-slot-number* **to** *end-slot-number*. The end slot number must be equal to or greater than the start slot number.

Usage guidelines

BootWare images are contained in the .bin Comware boot image file. You can specify a Comware boot image file in this command to upgrade the BootWares in the system before you upgrade the Comware images. If you do not upgrade BootWares before upgrading Comware images, the system automatically upgrades BootWares as necessary when loading Comware images.

The new BootWare images take effect after you reboot the device.

Examples

Use the file **a.bin** in the root directory of the flash memory to upgrade the BootWare image.

```
<Sysname> bootrom update file flash:/a.bin slot 1
   This command will update the Boot ROM file on the specified board(s), Continue? [Y/N]:y
   Now updating the Boot ROM, please wait.............Done.
```

Related commands

boot-loader file

display boot-loader

Use **display boot-loader** to display current software images and startup software images.

Syntax

display boot-loader [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies the member ID of an IRF member device. If you do not specify a member device, this command displays the software images on each IRF member device.

Examples

Display the current software images and startup software images.

```
<Sysname> display boot-loader
Software images on slot 1:
Current software images:
  flash:/boot.bin
  flash:/system.bin
  flash:/feature.bin
Main startup software images:
  flash:/boot.bin
  flash:/system.bin
  flash:/feature.bin
Backup startup software images:
  flash:/boot.bin
  flash:/system.bin
  flash:/feature.bin
```

Table 1 Command output

Field	Description
Current software images	Comware images that have been loaded.
Main startup software images	Primary Comware images for the next startup.
Backup startup software images	Backup Comware images for the next startup.

Related commands

boot-loader file

display install active

Use **display install active** to display active software images.

Syntax

display install active [**slot** *slot-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify an IRF member device, this command displays information for all IRF member devices.

verbose: Displays detailed information. If you do not specify this keyword, the command displays only image names.

Examples

Display brief information about active software images.

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot.bin
  flash:/system.bin
  flash:/feature.bin
```

Display detailed information about active software images.

```
<Sysname> display install active verbose
Active packages on slot 1:
flash:/boot.bin
 [Package]
 Vendor: H3C
 Product: s5130s-li
 Service name: boot
 Platform version: 7.1.022
 Product version: Test 2201
 Supported board: mpu
 [Component]
 Component: boot
```

```
 Description: boot package

flash:/system.bin
 [Package]
 Vendor: H3C
 Product: s5130s-li
 Service name: system
 Platform version: 7.1.022
 Product version: Test 2201
 Supported board: mpu
 [Component]
 Component: system
 Description: system package

flash:/feature.bin
 [Package]
 Vendor: H3C
 Product: s5130s-li
 Service name: test
 Platform version: 7.1.022
 Product version: Test 2201
 Supported board: mpu
 [Component]
 Component: test
 Description: test package
```

Table 2 Command output

Field	Description
[Package]	Detailed information about the software image.
Service name	Image type: • **boot**—Boot image. • **boot-patch**—Boot image patch. • **system**—System image. • **system-patch**—System image patch. • Any other value indicates a feature image.
Platform version	Platform software version.
Product version	Product software version.
Supported board	Device type supported by the software image. The value is fixed at **mpu**, which indicates an IRF member device.
[Component]	Information about components included in the image file.
Component	Component name.
Description	Component description.

Related commands

`install active`

display install committed

Use **display install committed** to display main startup software images.

Syntax

display install committed [**slot** *slot-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify an IRF member device, this command displays information for all IRF member devices.

verbose: Displays detailed information. If you do not specify this keyword, the command displays only image names.

Usage guidelines

Some **install** commands modify the current software image list but do not modify the main startup image list. For the software image changes to take effect after a reboot, you must execute the **install commit** command to update the main startup image list with the image changes. You can use the **display install committed** command to verify the operation results.

Both the **install commit** and **boot-loader file** commands modify the main startup software image list.

Examples

Display brief information about main startup software images.

```
<Sysname> display install committed
Committed packages on slot 1:
 flash:/boot-t5101.bin
 flash:/system-t5101.bin
 flash:/feature.bin
```

Display detailed information about main startup software images.

```
<Sysname> display install committed verbose
Committed packages on slot 1:
 flash:/boot-t5101.bin
 [Package]
 Vendor: H3C
 Product: s5130s-li
 Service name: boot
 Platform version: 7.1
 Product version: Beta 1330
 Supported board: mpu
 [Component]
 Component: boot
 Description: boot package
```

```
flash:/system-t5101.bin
[Package]
Vendor: H3C
Product: s5130s-li
Service name: system
Platform version: 7.1
Product version: Beta 1330
Supported board: mpu
[Component]
Component: system
Description: system package

flash:/ssh-feature.bin
[Package]
Vendor: H3C
Product: s5130s-li
Service name: ssh
Platform version: 7.1
Product version: Beta 1330
Supported board: mpu
[Component]
Component: ssh
Description: ssh package
```

For information about the command output, see Table 2.

Related commands

boot-loader file

install commit

install activate

Use **install activate** to activate feature or patch images.

Syntax

install activate feature *filename*&<1-30> **slot** *slot-number*

install activate patch *filename* { **all** | **slot** *slot-number* }

Views

User view

Predefined user roles

network-admin

Parameters

feature: Specifies a space-separated list of up to 30 feature image files.

patch: Specifies a patch image file. You can specify only one patch image file for the command at a time. However, you can execute the command multiple times to activate multiple patch image files.

filename: Specifies a .bin file in the *filesystemname*:/*filename*.**bin** format. The file must be stored in the root directory of a file system on the device. Excluding the file system location section (if any),

the value string can have a maximum of 63 characters. For more information about specifying a file, see file system management in *Fundamentals Configuration Guide*.

all: Specifies all IRF member devices.

slot *slot-number*: Specifies an IRF member device by its member ID.

Usage guidelines

This command activates images and adds the images to the current image list. Images run in memory immediately after they are activated. However, only images activated by using the **install activate patch** *filename* **all** command still run in memory after a reboot. For other images to take effect after a reboot, you must commit the software change by using the **install commit** command.

If the image file is not on the member device to be upgraded, the **install activate** command automatically copies the image file to the member device.

Examples

Activate **system-patch.bin** on IRF member device 1.

```
<Sysname> install activate system-patch.bin slot 1
```

Related commands

display install active

install commit

install deactivate

install commit

Use **install commit** to commit software changes.

Syntax

install commit

Views

User view

Predefined user roles

network-admin

Usage guidelines

This command adds the patch image file to the startup image list that the device used at startup.

- If the device used the main startup software image list at startup, this command adds the patch image file to the main startup software image list.
- If the device used the backup startup software image list at startup, this command adds the patch image file to the backup startup software image list.

Both the **install commit** and **boot-loader file** commands modify the main startup software image list. To modify the backup startup image list or add inactive images as main startup images, however, you must use the **boot-loader file** command.

For more information about main and backup startup software images, see *Fundamentals Configuration Guide*.

Examples

Commit software changes.

```
<Sysname> install commit
```

```
This operation will take several minutes, please wait.........................Done.
```

Related commands

`install activate`

`install deactivate`

install deactivate

Use **`install deactivate`** to deactivate feature or patch images.

Syntax

`install deactivate feature` *`filename`*&<1-30> **`slot`** *`slot-number`*

`install deactivate patch` *`filename`* { **`all`** | **`slot`** *`slot-number`* }

Views

User view

Predefined user roles

network-admin

Parameters

`feature`: Specifies a space-separated list of up to 30 feature image files.

`patch`: Specifies a patch image file. You can specify only one patch image file for the command at a time. However, you can execute the command multiple times to deactivate multiple patch image files.

`filename`: Specifies a .bin file in the *filesystemname*/*filename***.bin** format. The file must be stored in the root directory of a file system on the device. Excluding the file system location section (if any), the value string can have a maximum of 63 characters. For more information about specifying a file, see file system management in *Fundamentals Configuration Guide*.

`all`: Specifies all IRF member devices.

`slot` *`slot-number`*: Specifies an IRF member device by its member ID.

Usage guidelines

You can deactivate only active feature and patch images.

Images stop running in memory immediately after they are deactivated. However, only patch images deactivated by using the **`install deactivate patch`** *`filename`* **`all`** command do not run after a reboot. To prevent other deactivated images from running after a reboot, you must commit the software change by using the **`install commit`** command.

Examples

Deactivate **route-patch.bin** on IRF member device 1.

```
<Sysname> install deactivate patch flash:/route-patch.bin slot 1
```

Related commands

`display install active`

Contents

Device management commands

clock datetime

Use **clock datetime** to set the system time.

Syntax

clock datetime *time date*

Default

The system time is UTC time 00:00:00 01/01/2013.

Views

User view

Predefined user roles

network-admin

Parameters

time: Specifies a time in the *hh:mm:ss* format. The value range for *hh* is 0 to 23. The value range for *mm* is 0 to 59. The value range for *ss* is 0 to 59. The leading zero in a segment can be omitted. If the seconds segment is 0 (*hh*:*mm*:00), you can omit it. If both the minutes and seconds segments are 0 (*hh*:00:00), you can omit both of the segments. For example, to specify 08:00:00, you can enter 8.

date: Specifies a date in the *MM/DD/YYYY* or *YYYY/MM/DD* format. The value range for *YYYY* is 2000 to 2035. The value range for *MM* is 1 to 12. The value range for *DD* varies by month.

Usage guidelines

CAUTION:

This command changes the system time, which affects the execution of system time-related features (for example, scheduled tasks) and collaborative operations of the device with other devices (for example, log reporting and statistics collection). Before executing this command, make sure you fully understand its impact on your live network.

Correct system time is essential to network management and communication. You must configure the system time correctly before you run the device on the network.

For the device to use the local system time, execute the **clock protocol none** command and this command in turn. The specified system time takes effect immediately. Then, the device uses the clock signals generated by its built-in crystal oscillator to maintain the system time.

A device power cycling operation restores the local system time to the default. After the device is power cycled, you must execute this command again to set the local system time.

Examples

Set the system time to 08:08:08 01/01/2015.

```
<Sysname> clock datetime 8:8:8 1/1/2015
```

Set the system time to 08:10:00 01/01/2015.

```
<Sysname> clock datetime 8:10 2015/1/1
```

Related commands

clock protocol

clock summer-time

clock timezone

display clock

clock protocol

Use **clock protocol** to specify the system time source.

Use **undo clock protocol** to restore the default.

Syntax

clock protocol { **none** | **ntp** }

undo clock protocol

Default

The device obtains the UTC time from an NTP time source.

Views

System view

Predefined user roles

network-admin

Parameters

none: Uses the system time set by using the **clock datetime** command.

ntp: Uses NTP to obtain the UTC time. You must configure NTP correctly. For more information about NTP and NTP configuration, see *Network Management and Monitoring Configuration Guide*.

Usage guidelines

Correct system time is essential to network management and communication. You must configure the system time correctly before you run the device on the network.

The device can use the locally set system time, or obtain the UTC time from a time source on the network and calculate the system time.

If you execute the **clock protocol none** command, the device uses the locally set system time. The device then uses the clock signals generated by its built-in crystal oscillator to maintain the system time.

If you execute the **clock protocol ntp** command, the device obtains the UTC time through NTP and calculates the system time. The device then periodically synchronizes the UTC time and recalculates the system time.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure the device to use the local UTC time.

```
<Sysname> system-view
[Sysname] clock protocol none
```

clock summer-time

Use **clock summer-time** to set the daylight saving time.

Use **undo clock summer-time** to restore the default.

Syntax

clock summer-time *name* *start-time* *start-date* *end-time* *end-date* *add-time*

undo clock summer-time

Default

The daylight saving time is not set.

Views

System view

Predefined user roles

network-admin

Parameters

name: Specifies a name for the daylight saving time schedule, a case-sensitive string of 1 to 32 characters.

start-time: Specifies the start time in the *hh:mm:ss* format. The value range for *hh* is 0 to 23. The value range for *mm* is 0 to 59. The value range for *ss* is 0 to 59. The leading zero in a segment can be omitted. If the seconds segment is 0 (*hh*:*mm*:00), you can omit it. If both the minutes and seconds segments are 0 (*hh*:00:00), you can omit both of the segments. For example, to specify 08:00:00, you can enter 8.

start-date: Specifies the start date in one of the following formats:

- *MM/DD*. The value range for *MM* is 1 to 12. The value range for *DD* varies by month.
- *month week day*, where:
  - *month*—Takes **January**, **February**, **March**, **April**, **May**, **June**, **July**, **August**, **September**, **October**, **November** or **December**.
  - *week*—Represents week of the month. It takes **first**, **second**, **third**, **fourth**, **fifth**, or **last**.
  - *day*—Takes **Sunday**, **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, or **Saturday**.

end-time: Specifies the end time in the *hh:mm:ss* format. The value range for *hh* is 0 to 23. The value range for *mm* is 0 to 59. The value range for *ss* is 0 to 59. The leading zero in a segment can be omitted. If the seconds segment is 0 (*hh*:*mm*:00), you can omit it. If both the minutes and seconds segments are 0 (*hh*:00:00), you can omit both of the segments. For example, to specify 08:00:00, you can enter 8.

end-date: Specifies the end date in one of the following formats:

- *MM/DD*. The value range for *MM* is 1 to 12. The value range for *DD* varies by month.
- *month week day*, where:
  - *month*—Takes **January**, **February**, **March**, **April**, **May**, **June**, **July**, **August**, **September**, **October**, **November** or **December**.
  - *week*—Represents week of the month. It takes **first**, **second**, **third**, **fourth**, **fifth**, or **last**.
  - *day*—Takes **Sunday**, **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, or **Saturday**.

add-time: Specifies the time to be added to the standard time, in the *hh:mm:ss* format. The value range for *hh* is 0 to 23. The value range for *mm* is 0 to 59. The value range for *ss* is 0 to 59. The leading zero in a segment can be omitted. If the seconds segment is 0 (*hh*:*mm*:00), you can omit it. If both the minutes and seconds segments are 0 (*hh*:00:00), you can omit both of the segments. For example, to specify 08:00:00, you can enter 8.

Usage guidelines

Correct system time is essential to network management and communication. You must configure the system time correctly before you run the device on the network.

After you set the daylight saving time, the device recalculates the system time. To view the system time, use the **display clock** command.

Make sure all devices on the network are using the same daylight saving time as the local time.

Examples

Set the system time ahead 1 hour for the period between 06:00:00 on 08/01 and 06:00:00 on 09/01.

```
<Sysname> system-view
[Sysname] clock summer-time PDT 6 08/01 6 09/01 1
```

Related commands

clock datetime

clock timezone

display clock

clock timezone

Use **clock timezone** to set the time zone.

Use **undo clock timezone** to restore the default.

Syntax

clock timezone *zone-name* { **add** | **minus** } *zone-offset*

undo clock timezone

Default

The UTC time zone is used.

Views

System view

Predefined user roles

network-admin

Parameters

zone-name: Specifies a time zone by its name, a case-sensitive string of 1 to 32 characters.

add: Adds an offset to the UTC time.

minus: Decreases the UTC time by an offset.

zone-offset: Specifies an offset to the UTC time, in the *hh:mm:ss* format. The value range for *hh* is 0 to 23. The value range for *mm* is 0 to 59. The value range for *ss* is 0 to 59. The leading zero in a segment can be omitted. If the seconds segment is 0 (*hh*:*mm*:00), you can omit it. If both the minutes and seconds segments are 0 (*hh*:00:00), you can omit both of the segments. For example, to specify 08:00:00, you can enter 8.

Usage guidelines

Correct system time is essential to network management and communication. You must configure the system time correctly before you run the device on the network.

After you set the time zone, the device recalculates the system time. To view the system time, use the **display clock** command.

Make sure all devices on the network are using the same time zone as the local time.

Examples

Set the name of the time zone to **Z5**, and add 5 hours to the UTC time.

```
<Sysname> system-view
[Sysname] clock timezone Z5 add 5
```

Related commands

clock datetime

clock summer-time

display clock

command

Use **command** to assign a command to a job.

Use **undo command** to revoke a command.

Syntax

command *id command*

undo command *id*

Default

No command is assigned to a job.

Views

Job view

Predefined user roles

network-admin

Parameters

id: Specifies an ID for the command, in the range of 0 to 4294967295. A command ID uniquely identifies a command in a job. Commands in a job are executed in ascending order of their command IDs.

command: Specifies the command to be assigned to the job.

Usage guidelines

To assign a command (command A) to a job, you must first assign the job the command or commands for entering the view of command A.

If you specify the ID of an existing command for another command, the existing command is replaced.

Make sure all commands in a schedule are compliant to the command syntax. The system does not examine the syntax when you assign a command to a job.

If a command requires a yes or no answer, the system always assumes that a **Y** or **Yes** is entered. If a command requires a character string input, the system assumes that either the default character string (if any) or a null string is entered.

A job cannot contain the **telnet**, **ftp**, **ssh2**, or **monitor process** command.

Examples

Assign commands to the **backupconfig** job to back up the **startup.cfg** file to the TFTP server at 192.168.100.11.

```
<Sysname> system-view
[Sysname] scheduler job backupconfig
```

```
[Sysname-job-backupconfig] command 2 tftp 192.168.100.11 put flash:/startup.cfg
backup.cfg
```

Assign commands to the **shutdownGE** job to shut down GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] scheduler job shutdownGE
[Sysname-job-shutdownGE] command 1 system-view
[Sysname-job-shutdownGE] command 2 interface gigabitethernet 1/0/1
[Sysname-job-shutdownGE] command 3 shutdown
```

Related commands

scheduler job

copyright-info enable

Use **copyright-info enable** to enable copyright statement display.

Use **undo copyright-info enable** to disable copyright statement display.

Syntax

copyright-info enable

undo copyright-info enable

Default

Copyright statement display is enabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable copyright statement display.

```
<Sysname> system-view
[Sysname] copyright-info enable
```

The device will display the following statement when a user logs in:

```
**************************************************************************
* Copyright (c) 2004-2019 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                             *
* no decompiling or reverse-engineering shall be allowed.                *
**************************************************************************
```

display clock

Use **display clock** to display the system time, date, time zone, and daylight saving time.

Syntax

display clock

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the system time and date when the time zone is not specified.

```
<Sysname> display clock
10:09:00.258 UTC Fri 03/16/2015
```

The time is in the *hour*:*minute*:*second*.*milliseconds* format.

Display the system time and date when the time zone Z5 is specified.

```
<Sysname> display clock
15:10:00.152 Z5 Fri 03/16/2015
Time Zone : Z5 add 05:00:00
```

Display the system time and date when the time zone Z5 and daylight saving time PDT are specified.

```
<Sysname> display clock
15:11:00.211 Z5 Fri 03/16/2015
Time Zone : Z5 add 05:00:00
Summer Time : PDT 06:00:00 08/01 06:00:00 09/01 01:00:00
```

Related commands

clock datetime

clock timezone

clock summer-time

display copyright

Use **display copyright** to display the copyright statement.

Syntax

display copyright

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the copyright statement.

```
<Sysname> display copyright
...
```

display cpu-usage

Use **display cpu-usage** to display the current CPU usage statistics.

Syntax

display cpu-usage [**summary**] [**slot** *slot-number* [**cpu** *cpu-number* [**core** { *core-number*| **all** }]]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

summary: Displays CPU usage statistics in table form. If you do not specify this keyword, the command displays CPU usage statistics in text form.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays CPU usage statistics for all member devices.

cpu *cpu-number*: Specifies a CPU by its number.

core *core-number*: Specifies a CPU core by its number.

core all: Specifies all CPU cores.

Examples

Display the current CPU usage statistics in text form.

```
<Sysname> display cpu-usage
Slot 1 CPU 0 CPU usage:
       1% in last 5 seconds
       1% in last 1 minute
       1% in last 5 minutes
```

Display the current CPU usage statistics in table form.

```
<Sysname> display cpu-usage
Slot CPU        Last 5 sec        Last 1 min        Last 5 min
1    0          17%               29%               28%
```

Table 1 Command output

Field	Description
x% in last 5 seconds Last 5 sec	Average CPU or CPU core usage during the most recent 5-second interval.
y% in last 1 minute Last 1 min	Average CPU or CPU core usage during the most recent 1-minute interval.
z% in last 5 minutes Last 5 min	Average CPU or CPU core usage during the most recent 5-minute interval.

display cpu-usage configuration

Use **display cpu-usage configuration** to display CPU usage monitoring settings.

Syntax

display cpu-usage configuration [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the CPU usage monitoring settings for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Examples

Display the CPU usage monitoring settings.

```
<Sysname> display cpu-usage configuration
CPU usage monitor is enabled.
Current monitor interval is 60 seconds.
Current severe alarm threshold is 99%.
Current minor alarm threshold is 98%.
Current recovery-threshold is 50%.
```

Table 2 Command output

Field	Description
CPU usage monitor is *xxx*.	Whether CPU usage tracking is enabled.
Current monitor interval is *xxx*.	Sampling interval for CPU usage tracking.
Current severe alarm threshold is *xxx*.	Severe CPU usage alarm threshold.
Current minor alarm threshold is *xxx*.	Minor CPU usage alarm threshold.
Current recovery threshold is *xxx*.	CPU usage recovery threshold.

Related commands

monitor cpu-usage enable

monitor cpu-usage interval

monitor cpu-usage threshold

display cpu-usage history

Use **display cpu-usage history** to display the historical CPU usage statistics in a coordinate system.

Syntax

display cpu-usage history [**job** *job-id*] [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

job *job-id*: Specifies a process by its ID. The value range for *job-id* is 1 to 2147483647. If you do not specify a process, this command displays the statistics for the entire system's CPU usage (the total CPU usage of all processes). To view the IDs and names of the running processes, use the **display process** command. For more information, see *Network Management and Monitoring Configuration Guide*.

slot *slot-number*: Specifies an IRF member device by its member ID. If you specify a process but do not specify a member device, this command displays the statistics for the process on the master device. If you do not specify any options, this command displays the statistics for all processes on all member devices.

cpu *cpu-number*: Specifies a CPU by its number. If you specify a process but do not specify a CPU, this command displays the statistics for the default CPU. If you do not specify a process or CPU, this command displays the historical statistics for all CPUs.

Usage guidelines

After CPU usage monitoring is enabled, the system regularly samples CPU usage and saves the samples to the history record buffer. This command displays the most recent 60 samples in a coordinate system as follows:

The vertical axis represents the CPU usage. If a statistic is not a multiple of the usage step, it is rounded up or down to the closest multiple of the usage step. For example, if the CPU usage step is 5%, the statistic 53% is rounded up to 55%, and the statistic 52% is rounded down to 50%.

The horizontal axis represents the time.

Pound signs (#) indicate the CPU usage. The value on the vertical axis for the topmost pound sign at a specific time represents the CPU usage at that time.

Examples

Display the historical CPU usage statistics.

```
<Sysname> display cpu-usage history
100%|
 95%|
 90%|
 85%|
 80%|
 75%|
 70%|
 65%|
 60%|
 55%|
 50%|
 45%|
 40%|
 35%|
 30%|
 25%|
 20%|
 15%|             #
 10%|            ###  #
  5%|           ########
    ------------------------------------------------------------
              10        20        30        40        50        60  (minutes)
```

```
                    cpu-usage (Slot 1 CPU 0) last 60 minutes (SYSTEM)
```

The output shows the following items:

- Process name. The name **SYSTEM** represents the entire system.
- CPU that is holding the process: CPU 0 in slot 1.
- Historical CPU usage statistics for the entire system during the last 60 minutes.
  - **12 minutes ago**—Approximately 5%.
  - **13 minutes ago**—Approximately 10%.
  - **14 minutes ago**—Approximately 15%.
  - **15 minutes ago**—Approximately 10%.
  - **16 and 17 minutes ago**—Approximately 5%.
  - **18 minutes ago**—Approximately 10%.
  - **19 minutes ago**—Approximately 5%.
  - **Other time**—2% or lower.

Related commands

`monitor cpu-usage enable`

`monitor cpu-usage interval`

display device

Use **`display device`** to display device information.

Syntax

`display device`[**`flash`** | **`usb`**] [**`slot`** *`slot-number`* | **`verbose`**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

`flash`: Displays flash memory information.

`usb`: Displays USB interface information.

`slot` *`slot-number`*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices.

`verbose`: Displays detailed information. If you do not specify this keyword, this command displays brief information.

Usage guidelines

If you do not specify the **`flash`** and **`usb`** keywords, this command displays information about member devices.

Examples

Display device information.

```
<Sysname> display device
Slot 1
Slot Type             State    Subslot  Soft Ver            Patch Ver
```

```
1    S5130S-52S-HI    Master   0       S5130S-52S-HI6103P06 None
```

Table 3 Command output

Field	Description
Type	Device type.
State	Role of the device in an IRF fabric: • **Master**—The device is the master. • **Standby**—The device is a subordinate member.
Soft Ver	Software version of the device.
Patch Ver	Most recently released patch image version that is running on the device. If no patch image is installed, this field displays **None**. If both incremental and non-incremental patch images are running on the device, this field displays the most recently released incremental patch image version. For more information about patch image types, see software upgrade in *Fundamentals Configuration Guide*.

display device manuinfo

Use **display device manuinfo** to display electronic label information for the device.

Syntax

display device manuinfo [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays electronic label information for all member devices.

Usage guidelines

An electronic label contains the permanent configuration information, including the hardware serial number, manufacturing date, MAC address, and vendor name. The data is written to the storage component during hardware debugging or testing. This command displays only part of the electronic label information.

Examples

Display electronic label information for the device.

```
<Sysname> display device manuinfo
...
```

display device manuinfo power

Use **display device manuinfo power** to display electronic label information for a power supply.

Syntax

display device manuinfo slot *slot-number* **power** *power-id*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID.

power-id: Specifies a power supply by its ID.

Examples

Display electronic label information for a power supply.

```
<Sysname> display device manuinfo slot 1 power 1
...
```

display diagnostic-information

Use **display diagnostic-information** to display or save operating information for features and hardware modules.

Syntax

display diagnostic-information [**hardware** | **infrastructure** | **l2** | **l3** | **service**] [**key-info**] [*filename*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

hardware: Specifies hardware-related operating information.

infrastructure: Specifies operating information for the fundamental features.

l2: Specifies operating information for the Layer 2 features.

l3: Specifies operating information for the Layer 3 features.

service: Specifies operating information for Layer 4 and upper-layer features.

key-info: Displays or saves only critical operating information. The device might have a large amount of operating information if an exception occurs or after the device runs for a long period of time. Specifying this keyword reduces the command execution time and helps you focus on critical operating information. If you do not specify this keyword, the command displays or saves both critical and non-critical operating information.

filename: Saves the information to a file. The *filename* argument must use the **.tar.gz** extension. If you do not specify this argument, the command prompts you to choose whether to save the information to a file or display the information.

Usage guidelines

You can use one of the following methods to collect operating statistics for diagnostics and troubleshooting:

- Use separate **display** commands to collect operating information feature by feature or module by module.
- Use the **display diagnostic-information** command to collect operating information for multiple or all features and hardware modules.

To save storage space, this command automatically compresses the information before saving the information to a file. To view the file content:

1. Use the **tar extract** command to extract the file.
2. Use the **gunzip** command to decompress the extracted file.
3. Use the **more** command to view the content of the decompressed file.

If you abort the **display diagnostic-information** command, the **gunzip** command might not be able to decompress the extracted file. To decompress the extracted file, export the extracted file to a PC that is running Linux, and use the **gunzip -c** command.

If you do not specify a file name for the command, the system prompts you to choose whether to display or save the information. If you choose to save the information, the system automatically assigns a file name and displays the file name in brackets. For file name uniqueness, the file name includes the device name and the current system time. If the device name contains any of the following special characters, the system uses an underscore (_) to replace each special character: forward slashes (/), backward slashes (\), colons (:), asterisks (*), question marks (?), less than signs (<), greater than signs (>), pipeline signs (|), and quotation marks ("). For example, device name **A/B** will change to **A_B** in the file name, as in **flash:/diag_A_B_20160101-000438.tar.gz**.

If you do not specify any feature parameters, this command displays or saves the operating information for all features and modules.

This command does not support the |, **>**, and **>>** options.

While the device is executing this command, do not execute any other commands. Executing other commands might affect the collected operating information.

Examples

Display the operating information for all features and modules.

```
<Sysname> display diagnostic-information
Save or display diagnostic information (Y=save, N=display)? [Y/N]:n
================================================
  ===============display clock===============
14:03:55 UTC Thu 01/05/2015
================================================
  ===============display version===============
...
```

Save the operating information to the default file.

```
<Sysname> display diagnostic-information
Save or display diagnostic information (Y=save, N=display)? [Y/N]:y
Please input the file name(*.tar.gz)[flash:/diag_Sysname_20160101-024601.tar.gz]:
Diagnostic information is outputting to flash:/diag_Sysname_20160101-024601.tar.gz.
Please wait...
Save successfully.
```

Press **Enter** when the system prompts you to enter the file name.

Save the operating information for all features and modules to file **test.tar.gz**.

```
<Sysname> display diagnostic-information test.tar.gz
Diagnostic information is outputting to flash:/test.tar.gz.
Please wait...
Save successfully.
```

Related commands

gunzip

more

tar extract

display dying-gasp host

Use **display dying-gasp host** to display poweroff alarm destination host settings.

Syntax

display dying-gasp host

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display poweroff alarm destination host settings.

```
<Sysname> display dying-gasp host
IPv4 address: 1.1.1.0
Message type: SNMP Trap
Securityname: p1
Version: V1

IPv4 address: 1.1.1.1
Message type: Syslog
```

Table 4 Command output

Field	Description
IPv4 address	IPv4 address of the poweroff alarm destination host.
IPv6 address	IPv6 address of the poweroff alarm destination host.
Message type	Message types that the poweroff alarm destination host supports: • **SNMP Trap**—SNMP notification. • **Syslog**—Log message.
Securityname	SNMPv1 or SNMPv2c community name. This field is displayed when the message type is **SNMP Trap**.
Version	SNMP version: • **v1**—SNMPv1. • **v2c**—SNMPv2c. This field is displayed when the message type is **SNMP Trap**.

Related commands

dying-gasp host

display environment

Use **display environment** to display temperature information.

Syntax

display environment [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays temperature information for all member devices.

Examples

Display information about all temperature sensors on the device.

```
<Sysname> display environment
 System temperature information (degree centigrade):
 ---------------------------------------------------------------------
 Slot  Sensor    Temperature  Lower  Warning  Alarm  Shutdown
 1     hotspot 1 69           0      84       98     NA
 1     hotspot 2 67           0      84       98     NA
 1     hotspot 3 33           0      100      110    NA
 1     hotspot 4 33           0      100      110    NA
 1     hotspot 5 38           0      100      110    NA
 1     hotspot 6 36           0      100      110    NA
 1     hotspot 7 35           0      100      110    NA
 1     hotspot 8 42           0      100      110    NA
```

Table 5 Command output

Field	Description
System Temperature information (degree centigrade)	Temperature information (°C).
sensor	Temperature sensor: **hotspot**—Hotspot sensor.
Slot	Sensor position.
Temperature	Current temperature.
Lower	Lower temperature limit. If the device does not support this field, this field displays **NA**.
Warning	Warning temperature threshold. If the device does not support this field, this field displays **NA**.
Alarm	Alarming temperature threshold. If the device does not support this field,

Field	Description
	this field displays **NA**.
Shutdown	Shutdown temperature threshold. When the sensor temperature reaches the limit, the system shuts down automatically. If the device does not support this field, this field displays **NA**.

display fan

Use **display fan** to display fan tray operating status information.

Syntax

display fan [**slot** *slot-number* [*fan-id*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays fan tray operating status information for all member devices.

fan-id: Specifies a fan tray by its ID. If you do not specify a fan tray, this command displays operating status information for all fan trays at the specified position.

Examples

Display the operating states of all fan trays.

```
<Sysname> display fan
 Slot 1:
 Fan 1:
 State    : Normal
```

Table 6 Command output

Field	Description
Slot 1	Number of the member device.
Fan 1	Fan tray number.
State	Fan tray status: • **Absent**—The slot is not installed with a fan tray. • **Fault**—The fan tray is faulty. • **Normal**—The fan tray is operating correctly.

display memory

Use **display memory** to display memory usage information.

Syntax

display memory [**summary**] [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

summary: Displays brief information about memory usage. If you do not specify this keyword, the command displays detailed information about memory usage.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays memory usage for all member devices.

cpu *cpu-number*: Specifies a CPU by its number.

Examples

Display detailed memory usage information.

```
<Sysname> display memory
Memory statistics are measured in KB:
Slot 1:
             Total      Used      Free    Shared   Buffers    Cached   FreeRatio
Mem:        498284    293884    204400         0      1316     76332       41.0%
-/+ Buffers/Cache:    216236    282048
Swap:            0         0         0
```

Display brief memory usage information.

```
<Sysname> display memory summary
Memory statistics are measured in KB:
Slot CPU   Total      Used      Free      Buffers  Caches    FreeRatio
1    0     498284     293884    204400    1316     76332     41.0%
```

Table 7 Command output

Field	Description
Mem	Memory usage information.
Total	Total size of the physical memory space that can be allocated. The memory space is virtually divided into two parts. Part 1 is solely used for kernel code and kernel management functions. Part 2 can be allocated and used for such tasks as running service modules and storing files. The size of part 2 equals the total size minus the size of part 1.
Used	Used physical memory.
Free	Free physical memory.
Shared	Physical memory shared by processes. If this field is not supported, two hyphens (--) are displayed.
Buffers	Physical memory used for buffers. If this field is not supported, two hyphens (--) are displayed.
Cached Caches	Physical memory used for caches. If this field is not supported, two hyphens (--) are displayed.
FreeRatio	Free memory ratio.
-/+ Buffers/Cache	-/+ Buffers/Cache:used = Mem:Used – Mem:Buffers – Mem:Cached, which

Field	Description
	indicates the physical memory used by applications. -/+ Buffers/Cache:free = Mem:Free + Mem:Buffers + Mem:Cached, which indicates the physical memory available for applications.
Swap	Memory space for swapping.

display memory-threshold

Use **display memory-threshold** to display memory alarm thresholds and statistics.

Syntax

display memory-threshold [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the memory usage thresholds and statistics for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

For more information about memory usage notifications, see log information containing **MEM_EXCEED_THRESHOLD** or **MEM_BELOW_THRESHOLD**.

Examples

Display memory alarm thresholds and statistics.

```
<Sysname> display memory-threshold
Memory usage threshold: 100%
Free-memory thresholds:
    Minor: 60M
    Severe: 56M
    Critical: 52M
    Normal: 64M

Current free-memory state: Normal
Free-memory event statistics:
 [Back to normal state]
    First notification: 0.0
    Latest notification: 0.0
    Total number of notifications sent: 0
 [Entered minor alarm state]
    First notification at: 0.0
    Latest notification at: 0.0
    Total number of notifications sent: 0
 [Back to minor alarm state]
```

```
   First notification at: 0.0
   Latest notification at: 0.0
   Total number of notifications sent: 0
 [Entered severe alarm state]
   First notification at: 0.0
   Latest notification at: 0.0
   Total number of notifications sent: 0
 [Back to severe alarm state]
   First notification at: 0.0
   Latest notification at: 0.0
   Total number of notifications sent: 0
 [Entered critical alarm state]
   First notification at: 0.0
   Latest notification at: 0.0
   Total number of notifications sent: 0
```

display power

Use **display power** to display power supply information.

Syntax

display power [**slot** *slot-number* [*power-id*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays power supply information for all member devices.

power-id: Specifies a power supply by its ID. If you do not specify a power supply, this command displays information about all power supplies at the specified position.

Examples

Display power supply information.

```
<Sysname> display power
 Slot 1:
 PowerID State    Mode   Current(A)  Voltage(V)  Power(W)
 1       Absent   --        --          --          --
 2       Normal   AC        --          --          --
```

Table 8 Command output

Field	Description
PowerID	Power supply ID. On a device that supports only one power supply, you need to view only information about power supply 1.
State	Power supply status. • **Absent**—The slot is not installed with a hot-swappable power supply.

Field	Description
	• **Fault**—The power supply is faulty or is not powered on. • **Normal**—The power supply is operating correctly.
Mode	Mode of the power supply: • **AC**—AC power supply. • **DC**—DC power supply.
Current(A)	Output current of the power supply, in amperes. If this field is not supported, two hyphens (--) are displayed.
Voltage(V)	Output voltage of the power supply, in volts. If this field is not supported, two hyphens (--) are displayed.
Power(W)	Output power of the power supply, in watts. If this field is not supported, two hyphens (--) are displayed.

display scheduler job

Use **display scheduler job** to display job configuration information.

Syntax

display scheduler job [*job-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

job-name: Specifies a job by its name, a case-sensitive string of 1 to 47 characters. If you do not specify a job, this command displays configuration information for all jobs.

Examples

Display configuration information for all jobs.

```
<Sysname> display scheduler job
Job name: saveconfig
 copy startup.cfg backup.cfg

Job name: backupconfig

Job name: creat-VLAN100
 system-view
 vlan 100
```

// The output shows that the device has three jobs: the first has one command, the second does not have any commands, and the third has two commands. Jobs are separated by blank lines.

display scheduler logfile

Use **display scheduler logfile** to display job execution log information.

Syntax

display scheduler logfile

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display job execution log information.

```
<Sysname> display scheduler logfile
Logfile Size: 1902 Bytes.

Job name        : shutdown
Schedule name   : shutdown
Execution time  : Tue Dec 27 10:44:42 2015
Completion time : Tue Dec 27 10:44:47 2015
-------------------------------- Job output ---------------------------------
<Sysname>system-view
System View: return to User View with Ctrl+Z.
[Sysname]interface rang gigabitethernet 1/0/1 to gigabitethernet 1/0/3
[Sysname-if-range]shutdown
```

Table 9 Command output

Field	Description
Logfile Size	Size of the log file, in bytes.
Schedule name	Schedule to which the job belongs.
Execution time	Time when the job was started.
Completion time	Time when the job was completed. If the job has never been executed or the job does not have any commands, this field is blank.
Job output	Commands in the job and their output.

Related commands

reset scheduler logfile

display scheduler reboot

Use **display scheduler reboot** to display the automatic reboot schedule.

Syntax

display scheduler reboot

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the automatic reboot schedule.

```
<Sysname> display scheduler reboot
System will reboot at 16:32:00 05/23/2015 (in 1 hours and 39 minutes).
```

Related commands

scheduler reboot at

scheduler reboot delay

display scheduler schedule

Use **display scheduler schedule** to display schedule information.

Syntax

display scheduler schedule [*schedule-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

schedule-name: Specifies a schedule by its name, a case-sensitive string of 1 to 47 characters. If you do not specify a schedule, this command displays information about all schedules.

Examples

Display information about all schedules.

```
<Sysname> display scheduler schedule
Schedule name        : shutdown
Schedule type        : Run once after 0 hours 2 minutes
Start time           : Tue Dec 27 10:44:42 2015
Last execution time  : Tue Dec 27 10:44:42 2015
Last completion time : Tue Dec 27 10:44:47 2015
Execution counts     : 1
------------------------------------------------------------------------
Job name                                        Last execution status
shutdown                                        Successful
```

Table 10 Command output

Field	Description
Schedule type	Execution time setting of the schedule. If no execution time is specified, this field is not displayed.

Field	Description
Start time	Time to execute the schedule for the first time. If no execution time is specified, this field is not displayed.
Last execution time	Last time when the schedule was executed. If no execution time is specified, this field is not displayed. If the schedule has never been executed, "Yet to be executed" is displayed for this field.
Last completion time	Last time when the schedule was completed. If no execution time is specified, this field is not displayed.
Execution counts	Number of times the schedule has been executed. If the schedule has never been executed, this field is not displayed.
Job name	Name of a job under the schedule.
Last execution status	Result of the most recent execution: • **Successful**. • **Failed**. • **Waiting**—The device is executing the schedule and the job is waiting to be executed. • **In process**—The job is being executed. • **-NA-**—The execution time has not arrived yet. To view information about whether the commands in the job has been executed and the execution results, execute the **`display scheduler logfile`** command.

display system stable state

Use **`display system stable state`** to display system stability and status information.

Syntax

`display system stable state`

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

Before performing a switchover, execute this command multiple times to identify whether the system is operating stably. If the value of the **Redundancy Stable** field is not **Stable**, you cannot perform a switchover.

The device startup process takes some time. If the values of the status fields do not change to **Stable**, execute this command multiple times to identify the devices that are not in **Stable** state. You can also use other commands to identify the faulty components. For example:

- Use the **`display device`** command to identify the device operating status.
- Use the **`display system internal process state`** command in probe view to display service operating status.

Examples

Display system stability and status information.

```
<Sysname> display system stable state
System state    : Stable
```

```
Redundancy state: No redundance
  Slot   CPU   Role      State
 1      0     Active    Stable
```

Table 11 Command output

Field	Description
System state	System status: **Stable**—The system is operating stably.
Redundancy state	System redundancy status: • **Stable**—Member devices are operating stably. You can perform a switchover. • **No redundance**—The system has only one member device. You cannot perform a switchover. • **Not ready**—The system is not operating stably. You cannot perform a switchover.
Role	Role of the member device in the system: • **Active**—The member device is the master. • **Standby**—The member device is a subordinate member.
State	Member device status: • **Stable**—The member device is operating stably. • **Board inserted**—The member device has just been installed. • **Kernel initiating**—Member device kernel is being initialized. • **Service starting**—Services are starting on the member device. • **Service stopping**—Services are stopping on the member device. • **HA Batch backup**—An HA batch backup is going on. • **Interface data batch backup**—An interface data batch backup is in progress.
*	The object is not operating stably.

Related commands

`display device`

display transceiver alarm

Use **`display transceiver alarm`** to display transceiver alarms.

Syntax

`display transceiver alarm interface` [*`interface-type interface-number`*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

`interface` [*`interface-type interface-number`*]: Specifies an interface by its type and number. If no interface is specified, this command displays the alarms present on every transceiver module.

Usage guidelines

Table 12 shows the common transceiver alarm components. If no error occurs, "None" is displayed.

Table 12 Common transceiver alarm components

Field	Description
APD	Avalanche photo diode
PCS	Physical coding sublayer
PHY XS	PHY extended sublayer
PMA/PMD	Physical medium attachment/physical medium dependent
power	Optical power
REFCLK	Reference clock
RX	Receive
TEC	Thermoelectric cooler
Temp	Temperature
TX	Transmit
WIS	WAN interface sublayer

Examples

Display the alarms present on the transceiver module in interface GigabitEthernet 1/0/1.

```
<Sysname> display transceiver alarm interface gigabitethernet 1/0/1
GigabitEthernet1/0/1 transceiver current alarm information:
  RX loss of signal
  RX power low
```

Table 13 Command output

Field	Description
transceiver current alarm information	Alarms present on the transceiver module.
RX loss of signal	Received signals are lost.
RX power low	Received power is low.

display transceiver diagnosis

Use **`display transceiver diagnosis`** to display the current values of the digital diagnosis parameters on transceiver modules.

Syntax

`display transceiver diagnosis interface` [*`interface-type interface-number`*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface [*interface-type interface-number*]: Specifies an interface by its type and number. If no interface is specified, this command displays the current values of the digital diagnosis parameters on every transceiver module.

Examples

Display the current values of the digital diagnosis parameters on the transceiver module in interface GigabitEthernet 1/0/1.

```
<Sysname> display transceiver diagnosis interface gigabitethernet 1/0/1
GigabitEthernet1/0/1 transceiver diagnostic information:
  Current diagnostic parameters:
    Temp(°C)  Voltage(V)  Bias(mA)  RX power(dBm)  TX power(dBm)
    36        3.31        6.13      -35.64          -5.19
  Alarm thresholds:
            Temp(°C)   Voltage(V)  Bias(mA)  RX power(dBM)  TX power(dBM)
    High    50         3.55        1.44      -10.00         5.00
    Low     30         3.01        1.01      -30.00         0.00
```

Table 14 Command output

Field	Description
transceiver diagnostic information	Digital diagnosis information for the transceiver module in the interface.
Temp.(°C)	Temperature in °C, accurate to 1°C.
Voltage(V)	Voltage in V, accurate to 0.01 V.
Bias(mA)	Bias current in mA, accurate to 0.01 mA.
RX power(dBm)	Receive power in dBm, accurate to 0.01 dBm.
TX power(dBm)	Transmit power in dBm, accurate to 0.01 dBm.
High	High alarm threshold.
Low	Low alarm threshold.

display transceiver interface

Use **display transceiver interface** to display the key parameters of transceiver modules.

Syntax

display transceiver interface [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays the key parameters of every transceiver module.

Examples

Display the key parameters of the transceiver module in interface GigabitEthernet 1/0/1.

```
<Sysname> display transceiver interface gigabitethernet 1/0/1
...
```

display transceiver manuinfo

Use **display transceiver manuinfo** to display electronic label information for transceiver modules.

Syntax

display transceiver manuinfo interface [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface [*interface-type interface-number*]: Specifies an interface by its type and number. If no interface is specified, this command displays electronic label information for all transceiver modules.

Examples

Display electronic label information for the transceiver module in interface Ten-GigabitEthernet 1/0/49.

```
<Sysname> display transceiver manuinfo interface ten-gigabitethernet 1/0/49
...
```

display version

Use **display version** to display system version information.

Syntax

display version

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display system version information.

```
<Sysname> display version
H3C Comware Software, Version 7.1.070, Release 6309P01
Copyright (c) 2004-2019 New H3C Technologies Co., Ltd. All rights reserved.
H3C S5130S-52S-HI uptime is 0 weeks, 0 days, 6 hours, 43 minutes
```

```
Last reboot reason : Cold reboot

Boot image: flash:/s5130s_hi-cmw710-boot-r6309p01.bin
Boot image version: 7.1.070, Release 6309P01
  Compiled Jan 21 2019 11:00:00
System image: flash:/s5130s_hi-cmw710-system-r6309p01.bin
System image version: 7.1.070, Release 6309P01
  Compiled Jan 21 2019 11:00:00
...
```

Table 15 Command output

Field	Description
Last reboot reason	Reason for the last reboot: • **User reboot**—The reboot was manually initiated from a user interface, such as the CLI or SNMP. • **Cold reboot**—The reboot was caused by a power cycle. • **Kernel abnormality reboot**—The reboot was caused by kernel exceptions. • **DeadLoop reboot**—The reboot was caused by a kernel thread dead loop. • **DEV HandShake reboot**—The reboot was caused by a device management handshake failure. • **SlaveSwitch reboot**—The reboot was caused by a master/subordinate switchover. • **IRF Merge reboot**—The reboot was caused by an IRF merge. • **Auto Update reboot**—The reboot was caused by an automatic software upgrade. • **Memory exhaust reboot**—The reboot was caused by a card-memory-exhausted event.

display version-update-record

Use **`display version-update-record`** to display startup software image upgrade records.

Syntax

`display version-update-record`

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

The device records its current startup software version information whenever it starts up, and records all software version update information. Such information can survive reboots.

Examples

Display the startup software image upgrade records.

```
<Sysname> display version-update-record
Record 1  (updated on Apr 18 2019 at 06:23:54):
 *Name        : simware-cmw710-boot.bin
```

```
  Version     : 7.1.070 Release 6309P01
  Compile time: Mar 25 2019 15:52:43

 *Name        : simware-cmw710-system.bin
  Version     : 7.1.070 Release 6309P01
  Compile time: Mar 25 2019 15:52:43
```

Table 16 Command output

Field	Description
Record *n*	Number of the startup software image upgrade record. Record 1 is the most recent record.
Name	Software image file name.
*	The software image version changed during the upgrade.

Related commands

reset version-update-record

dying-gasp host

Use **dying-gasp host** to configure poweroff alarm destination host settings.

Use **undo dying-gasp host** to remove poweroff alarm destination host settings.

NOTE:

This command is supported only on the following devices:

- PoE devices and 52-port non-PoE devices.
- Devices that support hot-swappable power supplies.

Syntax

dying-gasp host { *ip-address* | **ipv6** *ipv6-address* } **snmp-trap version** { **v1** | **v2c** } **securityname** *security-string*

dying-gasp host { *ip-address* | **ipv6** *ipv6-address* } **syslog**

undo dying-gasp host { *ip-address* | **ipv6** *ipv6-address* } { **snmp-trap** | **syslog** }

Default

No poweroff alarm destination host settings are configured.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IPv4 address of the destination host to which the device sends the poweroff alarm.

ipv6 *ipv6-address*: Specifies the IPv6 address of the destination host to which the device sends the poweroff alarm.

snmp-trap: Uses an SNMP notification to send the poweroff alarm.

version: Specifies the SNMP version.

v1: Uses SNMPv1.

v2c: Uses SNMPv2c.

securityname *security-string*: Specifies an SNMPv1 or SNMPv2c community name, a case-sensitive string of 1 to 32 characters.

syslog: Uses a log message to send the poweroff alarm.

Usage guidelines

The device can send the poweroff alarm by using either or both of an SNMP notification and a log message.

The device can send the poweroff alarm to multiple destination hosts at the same time.

Examples

Configure the device to send the poweroff alarm to the host at 1.1.1.1 by using an SNMPv1 notification. The community name is **public**.

```
<Sysname> system-view
[Sysname] dying-gasp host 1.1.1.1 snmp-trap version v1 securityname public
```

Related commands

display dying-gasp host

dying-gasp source

dying-gasp source

Use **dying-gasp source** to specify the source interface for sending the poweroff alarm.

Use **undo dying-gasp source** to restore the default.

NOTE:

This command is supported only on the following devices:

- PoE devices and 52-port non-PoE devices.
- Devices that support hot-swappable power supplies.

Syntax

dying-gasp source *interface-type interface-number*

undo dying-gasp source

Default

No source interface is specified. On an IPv4 network, the device uses the primary IPv4 address of the output interface for the route to the destination host as the source address. On an IPv6 network, the device selects a source IPv6 address as defined in RFC 3484.

Views

System view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies a Layer 3 interface by its type and number.

Usage guidelines

The device uses the IPv6 address or primary IPv4 address of the specified source interface as the source address for outgoing poweroff alarm packets. The destination hosts use this address to identify SNMP notifications or log messages received from the device.

If no address is configured for the specified source interface, this command does not take effect. For this command to take effect, assign an address to the source interface.

Examples

Use the Loopback 1 interface as the source interface for sending the poweroff alarm.

```
<Sysname> system-view
[Sysname] dying-gasp source loopback 1
```

Related commands

dying-gasp host

header

Use **header** to configure a banner.

Use **undo header** to delete a banner.

Syntax

header { **legal** | **login** | **motd** | **shell** } *text*

undo header { **legal** | **login** | **motd** | **shell** }

Default

The device does not have banners.

Views

System view

Predefined user roles

network-admin

Parameters

legal: Configures the banner to be displayed before a user inputs the username and password to access the CLI.

login: Configures the banner to be displayed before password or scheme authentication is performed for a login user.

motd: Configures the greeting banner to be displayed before the legal banner appears.

shell: Configures the banner to be displayed before a user accesses user view.

text: Specifies the banner message. You can enter the banner message on the same line as the keywords or on different lines. For more information, see *Fundamentals Configuration Guide*.

Examples

Configure the legal banner.

```
<Sysname> system-view
[Sysname] header legal
Please input banner content, and quit with the character '%'.
```

```
Welcome to use the legal banner%
```

job

Use **job** to assign a job to a schedule.

Use **undo job** to revoke a job.

Syntax

job *job-name*

undo job *job-name*

Default

No job is assigned to a schedule.

Views

Schedule view

Predefined user roles

network-admin

Parameters

job-name: Specifies the job name, a case-sensitive string of 1 to 47 characters.

Usage guidelines

You can assign multiple jobs to a schedule. The jobs in a schedule are executed concurrently.

The jobs to be assigned to a schedule must already exist. To create a job, use the **scheduler job** command.

Examples

Assign job **save-job** to schedule **saveconfig**.

```
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] job save-job
```

Related commands

scheduler job

scheduler schedule

memory-threshold

Use **memory-threshold** to set free-memory thresholds.

Use **undo memory-threshold** to restore the defaults.

Syntax

memory-threshold [**slot** *slot-number* [**cpu** *cpu-number*]] [**ratio**] **minor** *minor-value* **severe** *severe-value* **critical** *critical-value* **normal** *normal-value*

undo memory-threshold [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

Minor alarm threshold: 60 MB.

Severe alarm threshold: 56 MB.

Critical alarm threshold: 52 MB.

Normal state threshold: 64 MB.

Views

System view

Predefined user roles

network-admin

Parameters

ratio: Specifies free-memory thresholds in percentage. If you do not specify this keyword, the command sets free-memory thresholds in MB.

minor *minor-value*: Specifies the minor alarm threshold. To view the value range for this threshold, enter a question mark (?) in the place of the *minor-value* argument. Setting this threshold to 0 disables the minor alarm feature.

severe *severe-value*: Specifies the severe alarm threshold. To view the value range for this threshold, enter a question mark (?) in the place of the *severe-value* argument. Setting this threshold to 0 disables the severe alarm feature.

critical *critical-value*: Specifies the critical alarm threshold. To view the value range for this threshold, enter a question mark (?) in the place of the *critical-value* argument. Setting this threshold to 0 disables the critical alarm feature.

normal *normal-value*: Specifies the normal state threshold. To view the value range for this threshold, enter a question mark (?) in the place of the *normal-value* argument.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command sets free-memory thresholds for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

To ensure correct operation and improve memory efficiency, the system monitors the amount of free memory space in real time. If the amount of free memory space decreases to or below the minor, severe, or critical alarm threshold, the system issues an alarm to affected service modules or processes.

If a memory alarm occurs, delete unused configuration items or disable some features to increase the free memory space. Because the memory space is insufficient, some configuration items might not be able to be deleted.

For more information about the thresholds, see *Fundamentals Configuration Guide*.

Examples

Set the minor alarm, severe alarm, critical alarm, and normal state thresholds to 64 MB, 48 MB, 32 MB, and 96 MB, respectively.

```
<Sysname> system-view
[Sysname] memory-threshold minor 64 severe 48 critical 32 normal 96
```

Set the minor alarm, severe alarm, critical alarm, and normal state thresholds to 3%, 2%, 1%, and 5% of the total memory size, respectively.

```
<Sysname> system-view
[Sysname] memory-threshold ratio minor 3 severe 2 critical 1 normal 5
```

Related commands

display memory-threshold

memory-threshold usage

Use **memory-threshold usage** to set the memory usage threshold.

Use **undo memory-threshold usage** to restore the default.

Syntax

memory-threshold [**slot** *slot-number* [**cpu** *cpu-number*]] **usage** *memory-threshold*

undo memory-threshold [**slot** *slot-number* [**cpu** *cpu-number*]] **usage**

Default

The memory usage threshold is 100%.

Views

System view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command sets the memory usage threshold for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

memory-threshold: Specifies the memory usage threshold in percentage. The value range is 0 to 100.

Usage guidelines

The device samples memory usage at 1-minute intervals. If the sample is greater than the memory usage threshold, the device sends a trap.

Examples

Set the memory usage threshold to 80%.

```
<Sysname> system-view
[Sysname] memory-threshold usage 80
```

Related commands

display memory-threshold

monitor cpu-usage enable

Use **monitor cpu-usage enable** to enable CPU usage monitoring.

Use **undo monitor cpu-usage enable** to disable CPU usage monitoring.

Syntax

monitor cpu-usage enable [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor cpu-usage enable [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

CPU usage monitoring is enabled.

Views

System view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command enables CPU usage monitoring for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

After CPU usage monitoring is enabled, the system samples and saves CPU usage at the interval specified by the **monitor cpu-usage interval** command. You can use the **display cpu-usage history** command to view recent CPU usage.

Examples

Enable CPU usage monitoring.

```
<Sysname> system-view
[Sysname] monitor cpu-usage enable
```

Related commands

display cpu-usage configuration

display cpu-usage history

monitor cpu-usage interval

monitor cpu-usage interval

Use **monitor cpu-usage interval** to set the sampling interval for CPU usage monitoring.

Use **undo monitor cpu-usage interval** to restore default settings.

Syntax

monitor cpu-usage interval *interval* [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor cpu-usage interval [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

The system samples CPU usage every 1 minute.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the sampling interval for CPU usage monitoring. Valid values include **5Sec** (5 seconds), **1Min** (1 minute), and **5Min** (5 minutes), case insensitive.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command sets the interval for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

After CPU usage monitoring is enabled, the system samples and saves CPU usage at the specified interval. You can use the **display cpu-usage history** command to view recent CPU usage.

Examples

Set the sampling interval for CPU usage monitoring to 5 seconds.

```
<Sysname> system-view
[Sysname] monitor cpu-usage interval 5Sec
```

Related commands

display cpu-usage configuration

display cpu-usage history

monitor cpu-usage enable

monitor cpu-usage threshold

Use **monitor cpu-usage threshold** to set CPU usage alarm thresholds.

Use **undo monitor cpu-usage threshold** to restore default settings.

Syntax

monitor cpu-usage threshold *severe-threshold* **minor-threshold** *minor-threshold* **recovery-threshold** *recovery-threshold* [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor cpu-usage threshold minor-threshold recovery-threshold [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

Severe CPU usage alarm threshold: 99%.

Minor CPU usage alarm threshold: 98%.

CPU usage recovery threshold: 50%.

Views

System view

Predefined user roles

network-admin

Parameters

severe-threshold: Specifies the severe CPU usage alarm threshold in percentage. The value range for this argument is 2 to 100.

minor-threshold *minor-threshold*: Specifies the minor CPU usage alarm threshold in percentage. The value range for this argument is 1 to the severe CPU usage alarm threshold minus 1.

recovery-threshold *recovery-threshold*: Specifies the CPU usage recovery threshold in percentage. The value range for this argument is 0 to the minor CPU usage alarm threshold minus 1.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command sets the CPU usage threshold for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

The device samples CPU usage at 1-minute intervals. If the sample is greater than the CPU usage threshold, the device sends a trap.

Examples

Set the severe CPU usage alarm threshold to 90%, minor CPU usage alarm threshold to 80%, and CPU usage recovery threshold to 70%.

```
<Sysname> system-view
[Sysname] monitor cpu-usage threshold 90 minor-threshold 80 recovery-threshold 70
```

Related commands

display cpu-usage configuration

monitor disk-usage disk

Use **monitor disk-usage disk** to set the disk usage threshold.

Use **undo monitor disk-usage disk** to restore the default.

NOTE:

This command is available only in Release 6348P01 and later.

Syntax

monitor disk-usage [**slot** *slot-number*] **disk** *disk-name* **threshold** *threshold-value*

undo monitor disk-usage [**slot** *slot-number*] **disk** *disk-name* **threshold**

Default

The disk usage threshold is 95%.

Views

System view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify an IRF member device, the command applies to the master device.

disk *disk-name*: Specifies a disk by its name. This option is case sensitive. The system will prompt a parameter error if you enter this option incorrectly.

threshold *threshold-value*: Specifies the disk usage threshold in percentage, in the range of 1 to 100.

Usage guidelines

After you configure the disk usage threshold, the device compares the usage of the disk with the threshold at each sampling. If the usage exceeds the threshold, the device sends a high disk usage alarm to the NETCONF module. For more information about the NETCONF module see *Network Management and Monitoring Configuration Guide*.

Examples

Set the disk usage threshold to 80%.

```
<Sysname> system-view
[Sysname] monitor disk-usage disk flash threshold 80
```

Related commands

monitor disk-usage interval

monitor disk-usage interval

Use **monitor disk-usage interval** to set the disk usage sampling interval.

Use **undo monitor disk-usage interval** to restore the default.

NOTE:
This command is available only in Release 6348P01 and later.

Syntax

monitor disk-usage interval *interval*

undo monitor disk-usage interval

Default

The disk usage sampling interval is 300 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval *interval-time*: Specifies the disk usage sampling interval in seconds, a multiple of five in the range of 5 to 1800.

Usage guidelines

After you set the disk usage sampling interval, the device samples disk usages at the specified intervals.

Examples

Set the disk usage sampling interval to 120 seconds.

```
<Sysname> system-view
[Sysname] monitor disk-usage interval 120
```

Related commands

monitor disk-usage disk

monitor resend cpu-usage

Use **monitor resend cpu-usage** to set CPU usage alarm resending intervals.

Use **undo monitor resend cpu-usage** to restore default settings.

Syntax

monitor resend cpu-usage { **minor-interval** *minor-interval* | **severe-interval** *severe-interval* } * [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor resend cpu-usage [**minor-interval** | **severe-interval**] [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

The minor alarm resending interval is 300 seconds. The severe alarm resending interval is 60 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

minor-interval *minor-interval*: Specifies the minor alarm resending interval in seconds, a multiple of five in the range of 10 to 3600.

severe-interval *severe-interval*: Specifies the severe alarm resending interval in seconds, a multiple of five in the range of 10 to 3600.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command sets alarm resending intervals for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

The device samples CPU usage periodically and compares the sample with the CPU usage threshold. If the sample increases above an alarm threshold, the CPU usage enters an alarm state and the device sends an alarm.

While the CPU usage is in minor alarm state, the device sends minor alarms periodically until the CPU usage increases above the severe threshold or the minor alarm is removed.

While the CPU usage is in severe alarm state, the device sends severe alarms periodically until the severe alarm is removed.

You can use this command to change CPU usage alarm resending intervals.

If you do not specify the **minor-interval** or **severe-interval** keyword, the **undo monitor resend cpu-usage** command restores default settings for both the minor and severe alarm resending intervals.

Examples

Set the CPU usage minor alarm resending interval to 60 seconds for CPU 0 in slot 1.

```
<Sysname> system-view
[Sysname] monitor resend cpu-usage minor-interval 60 slot 1 cpu 0
```

monitor resend memory-threshold

Use **monitor resend memory-threshold** to set memory depletion alarm resending intervals.

Use **undo monitor resend memory-threshold** to restore default settings.

Syntax

monitor resend memory-threshold { **critical-interval** *critical-interval* | **minor-interval** *minor-interval* | **severe-interval** *severe-interval* } * [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor resend memory-threshold [**critical-interval** | **minor-interval** | **severe-interval**] * [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

- Minor alarm resending interval: 12 hours.
- Severe alarm resending interval: 3 hours.
- Critical alarm resending interval: 1 hour.

Views

System view

Predefined user roles

network-admin

Parameters

critical-interval *critical-interval*: Specifies the critical alarm resending interval in hours, in the range of 1 to 48.

minor-interval *minor-interval*: Specifies the minor alarm resending interval in hours, in the range of 1 to 48.

severe-interval *severe-interval*: Specifies the severe alarm resending interval in hours, in the range of 1 to 48.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command sets alarm resending intervals for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

The device samples the amount of free memory space periodically and compares the sample with free-memory thresholds. If the sample decreases to or below a threshold, the device enters a memory depletion alarm state and sends an alarm.

In critical alarm state, the device sends critical alarm notifications periodically until the critical alarm is removed.

In a lower alarm state, the device sends notifications for the alarm state periodically until it enters a higher alarm state or the current alarm is removed.

You can use this command to change the alarm resending intervals.

If you do not specify any memory depletion alarm resending intervals, the **undo monitor resend memory-threshold** command restores default settings for all memory depletion alarm resending intervals.

Examples

Set the minor memory depletion alarm resending interval to 12 hours for CPU 0 in slot 1.

```
<Sysname> system-view
[Sysname] monitor resend memory-threshold minor-interval 12 slot 1 cpu 0
```

password-recovery enable

Use **password-recovery enable** to enable password recovery capability.

Use **undo password-recovery enable** to disable password recovery capability.

Syntax

password-recovery enable

undo password-recovery enable

Default

Password recovery capability is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Password recovery capability controls console user access to the device configuration and SDRAM from BootWare menus.

If password recovery capability is enabled, a console user can access the device configuration without authentication to configure new passwords.

If password recovery capability is disabled, console users must restore the factory-default configuration before they can configure new passwords. Restoring the factory-default configuration deletes the next-startup configuration files.

To enhance system security, disable password recovery capability.

Availability of BootWare menu options depends on the password recovery capability setting. For more information, see the release notes.

Examples

Disable password recovery capability.

```
<Sysname> system-view
[Sysname] undo password-recovery enable
```

reboot

Use **reboot** to reboot the device.

Syntax

reboot [**slot** *slot-number*] [**force**]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify an IRF member device, the command reboots all IRF member devices.

force: Reboots the device immediately without performing software or hard disk check. If this keyword is not specified, the system first identifies whether the reboot might result in data loss or a system failure. For example, the system identifies whether the main system software image file exists and whether a write operation is in progress on a storage medium. If the reboot might cause problems, the system does not reboot the device.

Usage guidelines

CAUTION:

- A reboot might interrupt network services.
- Use the **force** keyword only when the device fails or a **reboot** command without the **force** keyword cannot perform a reboot correctly. A **reboot** command with the **force** keyword might result in file system corruption because it does not perform data protection.

If the main startup software images are corrupt or missing, you must re-specify a set of main startup software images before executing the **reboot** command.

For data security, the device does not reboot if you reboot the device while the device is performing file operations.

If the IRF fabric has only one member device, rebooting the member device reboots the entire IRF fabric. If the IRF fabric has a subordinate member and the member is operating correctly, rebooting the master triggers a master/subordinate switchover.

To ensure correct operation of the IRF fabric and member devices, do not trigger a switchover by rebooting the master if no subordinate member devices are in **Stable** state. To view the status of subordinate member devices, execute the **display system stable state** command.

Examples

Reboot the device. Save the running configuration at prompt.

```
<Sysname> reboot
Start to check configuration with next startup configuration file, please
wait.........DONE!
Current configuration will be lost after the reboot, save current configuration? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Configuration is saved to mainboard device successfully.
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait...
```

Reboot the device immediately without performing software check.

```
<Sysname> reboot force
A forced reboot might cause the storage medium to be corrupted. Continue? [Y/N]:y
Now rebooting, please wait...
```

Related commands

display system stable state

reset scheduler logfile

Use **reset scheduler logfile** to clear job execution log information.

Syntax

reset scheduler logfile

Views

User view

Predefined user roles

network-admin

Examples

Clear job execution log information.

```
<Sysname> reset scheduler logfile
```

Related commands

display scheduler logfile

reset version-update-record

Use **reset version-update-record** to clear startup software image upgrade records.

Syntax

reset version-update-record

Views

System view

Predefined user roles

network-admin

Examples

Clear the startup software image upgrade records.

```
<Sysname> system-view
[Sysname] reset version-update-record
This command will delete all records of version update. Continue? [Y/N]:y
```

Related commands

display version-update-record

restore factory-default

Use **restore factory-default** to restore the factory-default configuration for the device.

Syntax

restore factory-default

Views

User view

Predefined user roles

network-admin

Usage guidelines

CAUTION:
This command restores the device to the factory default settings. Use this command with caution.

This command is disruptive. Use this command only when you cannot troubleshoot the device by using other methods, or you want to use the device in a different scenario.

Examples

Restore the factory-default configuration for the device.

```
<Sysname> restore factory-default
This command will restore the system to the factory default configuration and clear the
operation data. Continue [Y/N]:y
Restoring the factory default configuration. This process might take a few minutes. Please
wait.....................................................................
.....................Done.
Please reboot the system to place the factory default configuration into effect.
```

Related commands

reboot

scheduler job

Use **scheduler job** to create a job and enter its view, or enter the view of an existing job.

Use **undo scheduler job** to delete a job.

Syntax

scheduler job *job-name*

undo scheduler job *job-name*

Default

No job exists.

Views

System view

Predefined user roles

network-admin

Parameters

job-name: Specifies the job name, a case-sensitive string of 1 to 47 characters.

Usage guidelines

A job can be referenced by multiple schedules. In job view, you can assign commands to the job.

Examples

Create a job named **backupconfig** and enter job view.

```
<Sysname> system-view
[Sysname] scheduler job backupconfig
[Sysname-job-backupconfig]
```

Related commands

command

scheduler schedule

scheduler logfile size

Use **scheduler logfile size** to set the size of the job execution log file.

Syntax

scheduler logfile size *value*

Default

The size of the job execution log file is 16 KB.

Views

System view

Predefined user roles

network-admin

Parameters

value: Specifies the size of the job execution log file, in KB. The value range is 16 to 1024.

Usage guidelines

The job execution log file saves the execution information of jobs. If the file is full, old records are deleted to make room for new records. If the size of the log information to be written to the file is greater than the file size, the excessive information is not written to the file.

Examples

Set the size of the job execution log file to 32 KB.

```
<Sysname> system-view
[Sysname] scheduler logfile size 32
```

Related commands

display scheduler logfile

scheduler reboot at

Use **scheduler reboot at** to specify the reboot date and time.

Use **undo scheduler reboot** to delete the reboot schedule configuration.

Syntax

scheduler reboot at *time* [*date*]

undo scheduler reboot

Default

No reboot date or time is specified.

Views

User view

Predefined user roles

network-admin

Parameters

time: Specifies the reboot time in the *hh:mm* format. The value range for *hh* is 0 to 23. The value range for *mm* is 0 to 59.

date: Specifies the reboot date in the *MM/DD/YYYY* or *YYYY/MM/DD* format. The value range for *YYYY* is 2000 to 2035. The value range for *MM* is 1 to 12. The value range for *DD* varies by month.

Usage guidelines

CAUTION:

This command enables the device to reboot at a scheduled time, which causes service interruption. Before executing this command, make sure you fully understand its impact on your live network.

When the *date* argument is not specified, the system uses the following rules to determine the reboot time:

- If the reboot time is later than the current time, a reboot occurs at the reboot time of the current day.
- If the reboot time is earlier than the current time, a reboot occurs at the reboot time the next day.

The device supports only one device reboot schedule. If you execute both the **scheduler reboot delay** and **scheduler reboot at** commands or execute one of the commands multiple times, the most recent configuration takes effect.

For data security, the system does not reboot at the reboot time if a file operation is being performed.

Examples

Configure the device to reboot at 12:00 p.m. This example assumes that the current time is 11:43 a.m. on June 6, 2015.

```
<Sysname> scheduler reboot at 12:00
Reboot system at 12:00:00 06/06/2015 (in 0 hours and 16 minutes). Confirm? [Y/N]:
```

Related commands

scheduler reboot delay

scheduler reboot delay

Use **scheduler reboot delay** to specify the reboot delay time.

Use **undo scheduler reboot** to delete the reboot schedule configuration.

Syntax

scheduler reboot delay *time*

undo scheduler reboot

Default

No reboot delay time is specified.

Views

User view

Predefined user roles

network-admin

Parameters

time: Specifies the reboot delay time in the *hh:mm* or *mm* format. This argument can contain up to six characters. When in the *hh:mm* format, *mm* must be in the range of 0 to 59.

Usage guidelines

CAUTION:

This command enables the device to reboot after a delay, which causes service interruption. Before executing this command, make sure you fully understand its impact on your live network.

The device supports only one device reboot schedule. If you execute both the **scheduler reboot delay** and **schedule reboot at** commands or execute one of the commands multiple times, the most recent configuration takes effect.

For data security, the system does not reboot at the reboot time if a file operation is being performed.

Examples

Configure the device to reboot after 88 minutes. This example assumes that the current time is 11:48 a.m. on June 6, 2015.

```
<Sysname> scheduler reboot delay 88
Reboot system at 13:16 06/06/2015(in 1 hours and 28 minutes). Confirm? [Y/N]:
```

scheduler schedule

Use **scheduler schedule** to create a schedule and enter its view, or enter the view of an existing schedule.

Use **undo scheduler schedule** to delete a schedule.

Syntax

scheduler schedule *schedule-name*

undo scheduler schedule *schedule-name*

Default

No schedule exists.

Views

System view

Predefined user roles

network-admin

Parameters

schedule-name: Specifies the schedule name, a case-sensitive string of 1 to 47 characters.

Usage guidelines

You can configure a schedule to have the device automatically run a command or a set of commands without administrative interference.

To configure a schedule:

1. Use the **scheduler job** command to create a job and enter job view.
2. Use the **command** command to assign commands to the job.
3. Use the **scheduler schedule** command to create a schedule and enter schedule view.
4. Use the **job** command to assign the job to the schedule. You can assign multiple jobs to a schedule. The jobs must already exist.
5. Use the **user-role** command to assign user roles to the schedule. You can assign up to 64 user roles to a schedule.
6. Use the **time at**, **time once**, or **time repeating** command to specify an execution time for the schedule. You can specify only one execution time for a schedule.

Examples

Create a schedule named **saveconfig**.

```
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
```

Related commands

job

time at

time once

shutdown-interval

Use **shutdown-interval** to set the port status detection timer.

Use **undo shutdown-interval** to restore the default.

Syntax

shutdown-interval *interval*

undo shutdown-interval

Default

The port status detection timer setting is 30 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the port status detection timer value in seconds. In a version earlier than Release 6333, the value range is 0 to 300. In Release 6333 and later, the value range is 0 to 3600. To disable port status detection, set this argument to 0.

Usage guidelines

The device starts a port status detection timer when a port is shut down by a protocol. Once the timer expires, the device brings up the port so the port status reflects the port's physical status.

If you change the timer setting during port detection, the device compares the new setting (T1) with the time that elapsed since the port was shut down (T).

If T < T1, the port will be brought up after T1 – T seconds.

If T ≥ T1, the port is brought up immediately.

For example, the timer setting is 30 seconds. If you change it to 10 seconds 2 seconds after the port is shut down, the port will come up 8 seconds later. If you change the timer setting to 2 seconds 10 seconds after the port is shut down, the port comes up immediately.

Examples

Set the port status detection timer to 100 seconds.

```
<Sysname> system-view
[Sysname] shutdown-interval 100
```

sysname

Use **sysname** to set the device name.

Use **undo sysname** to restore the default.

Syntax

sysname *sysname*

undo sysname

Default

The device name is H3C.

Views

System view

Predefined user roles

network-admin

Parameters

sysname: Specifies a name for the device, a string of 1 to 64 characters.

Usage guidelines

A device name identifies a device in a network and is used in CLI view prompts. For example, if the device name is **Sysname**, the user view prompt is <Sysname>.

Examples

Set the name of the device to **R2000**.

```
<Sysname> system-view
[Sysname] sysname R2000
[R2000]
```

transceiver monitor enable

Use **transceiver monitor enable** to enable transceiver monitoring.

Use **undo transceiver monitor enable** to restore the default.

NOTE:
This command is available only in 6343P08 and later.

Syntax

transceiver monitor enable

undo transceiver monitor enable

Default

Transceiver monitoring is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

After transceiver monitoring is enabled, the device samples the parameters of transceiver modules periodically, including the input power and output power of transceiver modules. If a sampled value reaches the alarm threshold, the device generates a log to notify users.

Examples

Enable transceiver monitoring.

```
<Sysname> system-view
[Sysname] transceiver monitor enable
```

Related commands

transceiver monitor interval

transceiver monitor interval

Use **transceiver monitor interval** to set a transceiver monitoring interval.

Use **undo transceiver monitor interval** to restore the default.

NOTE:

This command is available only in 6343P08 and later.

Syntax

transceiver monitor interval *interval*

undo transceiver monitor interval

Default

The transceiver monitoring interval is 600 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the transceiver monitoring interval in seconds, in the range of 300 to 3600.

Usage guidelines

After transceiver monitoring is enabled, the device samples the parameters of transceiver modules periodically, including the input power and output power of transceiver modules. If a sampled value reaches the alarm threshold, the device generates a log entry to notify users.

This command takes effect only when the **transceiver monitor enable** command is used.

Examples

Set the transceiver monitoring interval to 500 seconds.

```
<Sysname> system-view
[Sysname] transceiver monitor interval 500
```

Related commands

transceiver monitor enable

temperature-limit

Use **temperature-limit** to set the temperature alarm thresholds.

Use **undo temperature-limit** to restore the default.

Syntax

temperature-limit slot *slot-number* **hotspot** *sensor-number lowlimit warninglimit* [*alarmlimit*]

undo temperature-limit slot *slot-number* **hotspot** *sensor-number*

Default

The defaults vary by temperature sensor model. To view the defaults, execute the **undo temperature-limit** and **display environment** commands in turn.

Views

System view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID.

hotspot: Configures temperature alarm thresholds for hotspot sensors. A hotspot sensor is typically near the chip that generates a great amount of heat and used to monitor the chip.

sensor-number: Specifies a sensor by its number. To view the value range, enter a question mark (?) in the place of this argument.

lowlimit: Specifies the low-temperature threshold in Celsius degrees. The value range varies by temperature sensor. To view the value range, enter a question mark (?) in the place of this argument.

warninglimit: Specifies the high-temperature warning threshold in Celsius degrees. This threshold must be greater than the low-temperature threshold. To view the value range, enter a question mark (?) in the place of this argument.

alarmlimit: Specifies the high-temperature alarming threshold in Celsius degrees. This threshold must be greater than the warning threshold. To view the value range, enter a question mark (?) in the place of this argument.

Usage guidelines

When the device temperature drops below the low-temperature threshold or reaches the high-temperature warning or alarming threshold, the device performs the following operations:

- Sends log messages and traps.
- Sets LEDs on the device panel.

Examples

Set temperature alarm thresholds for hotspot sensor 1 in a slot.

```
<Sysname> system-view
[Sysname] temperature-limit slot 1 hotspot 1 -10 50 60
```

Related commands

display environment

time at

Use **time at** to specify an execution date and time for a non-periodic schedule.

Use **undo time** to delete the execution date and time configuration for a non-periodic schedule.

Syntax

time at *time date*

undo time

Default

No execution time or date is specified for a non-periodic schedule.

Views

Schedule view

Predefined user roles

network-admin

Parameters

time: Specifies the schedule execution time in the *hh:mm* format. The value range for *hh* is 0 to 23. The value range for *mm* is 0 to 59.

date: Specifies the schedule execution date in the *MM/DD/YYYY* or *YYYY/MM/DD* format. The value range for *YYYY* is 2000 to 2035. The value range for *MM* is 1 to 12. The value range for *DD* varies by month.

Usage guidelines

The specified time (date plus time) must be later than the current system time.

The **time at** command, the **time once** command, and the **time repeating** command overwrite one another. The most recently executed command takes effect.

Examples

Configure the device to execute schedule **saveconfig** at 01:01 a.m. on May 11, 2015.

```
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] time at 1:1 2015/05/11
```

Related commands

scheduler schedule

time once

Use **time once** to specify one or more execution days and the execution time for a non-periodic schedule.

Use **undo time** to delete the execution day and time configuration for a non-periodic schedule.

Syntax

time once at *time* [**month-date** *month-day* | **week-day** *week-day*&<1-7>]

time once delay *time*

undo time

Default

No execution time or day is specified for a non-periodic schedule.

Views

Schedule view

Predefined user roles

network-admin

Parameters

at *time*: Specifies the execution time in the *hh:mm* format. The value range for *hh* is 0 to 23. The value range for *mm* is 0 to 59.

month-date *month-day*: Specifies a day in the current month, in the range of 1 to 31. If you specify a day that does not exist in the current month, the configuration takes effect on that day in the next month.

week-day *week-day*&<1-7>: Specifies a space-separated list of up to seven week days for the schedule. Valid week day values include **Mon**, **Tue**, **Wed**, **Thu**, **Fri**, **Sat**, and **Sun**.

delay *time*: Specifies the delay time for executing the schedule, in the *hh:mm* or *mm* format. This argument can have up to six characters. When in the *hh:mm* format, *mm* must be in the range of 0 to 59.

Usage guidelines

If the specified time has already occurred, the schedule will be executed at the specified time the following day.

If the day in the month has already occurred, the schedule will be executed at the specified day in the following month.

If the specified day in a week has already occurred, the schedule will be executed at the specified day in the following week.

The **time at** command, the **time once** command, and the **time repeating** command overwrite one another. The most recently executed command takes effect.

Examples

Configure the device to execute schedule **saveconfig** once at 15:00.

```
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] time once at 15:00
Schedule starts at 15:00 5/11/2011.
```

Configure the device to execute schedule **saveconfig** once at 15:00 on the coming 15th day in a month.

```
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] time once at 15:00 month-date 15
```

Configure the device to execute schedule **saveconfig** at 12:00 p.m. on the coming Monday and Friday.

```
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] time once at 12:00 week-day mon fri
```

Configure the device to execute schedule **saveconfig** after 10 minutes.

```
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] time once delay 10
```

Related commands

scheduler schedule

time repeating

Use **time repeating** to specify an execution time table for a periodic schedule.

Use **undo time** to delete the execution time table configuration for a periodic schedule.

Syntax

time repeating [**at** *time* [*date*]] **interval** *interval*

time repeating at *time* [**month-date** [*month-day* | **last**] | **week-day** *week-day*&<1-7>]

undo time

Default

No execution time table is specified for a periodic schedule.

Views

Schedule view

Predefined user roles

network-admin

Parameters

at *time*: Specifies the execution time in the *hh:mm* format. The value range for *hh* is 0 to 23. The value range for *mm* is 0 to 59. If you do not specify this option, the current system time is used as the execution time.

date: Specifies the start date for the periodic schedule, in the *MM/DD/YYYY* or *YYYY/MM/DD* format. The value range for *YYYY* is 2000 to 2035. The value range for *MM* is 1 to 12. The value range for *DD* varies by month. If you do not specify this argument, the execution start date is the first day when the specified time arrives.

interval *interval*: Specifies the execution time interval in the *hh:mm or mm* format. This argument can have up to six characters. When in the *hh:mm* format, *mm* must be in the range of 0 to 59. When in the *mm* format, this argument must be equal to or greater than 1 minute.

month-date [*month-day* | **last**]: Specifies a day in a month, in the range 1 to 31. The **last** keyword indicates the last day of a month. If you specify a day that does not exist in a month, the configuration takes effect on that day in the next month.

week-day *week-day*&<1-7>: Specifies a space-separated list of up to seven week days for the schedule. Valid week day values include **Mon**, **Tue**, **Wed**, **Thu**, **Fri**, **Sat**, and **Sun**.

Usage guidelines

The **time repeating** [**at** *time* [*date*]] **interval** *interval* command configures the device to execute a schedule at intervals from the specified time on.

The **time repeating at** *time* [**month-date** [*month-day* | **last**] | **week-day** *week-day*&<1-7>] command configures the device to execute a schedule at the specified time on every specified day in a month or week.

The **time at** command, the **time once** command, and the **time repeating** command overwrite one another, whichever is executed most recently takes effect.

Examples

Configure the device to execute schedule **saveconfig** once an hour from 8:00 a.m. on.

```
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] time repeating at 8:00 interval 60
```

Configure the device to execute schedule **saveconfig** at 12:00 p.m. every day.

```
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] time repeating at 12:00
```

Configure the device to execute schedule **saveconfig** at 8:00 a.m. on the 5th of every month.

```
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] time repeating at 8:00 month-date 5
```

Configure the device to execute schedule **saveconfig** at 8:00 a.m. on the last day of every month.

```
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] time repeating at 8:00 month-date last
```

Configure the device to execute schedule **saveconfig** at 8:00 a.m. every Friday and Saturday.

```
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] time repeating at 8:00 week-day fri sat
```

Related commands

scheduler schedule

user-role

Use **user-role** to assign user roles to a schedule.

Use **undo user-role** to remove user roles from a schedule.

Syntax

user-role *role-name*

undo user-role *role-name*

Default

A schedule has the user roles of the schedule creator.

Views

Schedule view

Predefined user roles

network-admin

Parameters

role-name: Specifies a user role name, a case-sensitive string of 1 to 63 characters. The user role can be user-defined or predefined. Predefined user roles include network-admin, network-operator, and level-0 to level-15.

Usage guidelines

A schedule must have one or more user roles. A command in a schedule can be executed if it is permitted by one or more user roles of the schedule. For more information about user roles, see the RBAC configuration in *Fundamentals Configuration Guide*.

A schedule can have a maximum of 64 user roles. After the limit is reached, you cannot assign additional user roles to the schedule.

Examples

Assign user role **rolename** to schedule **test**.

```
<Sysname> system-view
[Sysname] scheduler schedule test
[Sysname-schedule-test] user-role rolename
```

Related commands

command

scheduler schedule

Contents

Tcl commands

cli

Use **cli** to enable a Comware command to be executed in Tcl configuration view when it conflicts with a Tcl command.

Syntax

cli *command*

Views

Tcl configuration view

Predefined user roles

network-admin

Parameters

command: Specifies the commands to be executed. They must be complete command lines.

Usage guidelines

In Tcl configuration view, if a Comware command conflicts with a Tcl command, the Tcl command will be executed. To execute the Comware command when a conflict occurs, execute the **cli** command.

Examples

Perform the following steps to execute a Comware command that conflicts with a Tcl command in Tcl configuration view.

1. Execute a Comware command in Tcl configuration view. The output shows that the Comware command cannot be executed because it conflicts with a Tcl command.

```
<Sysname> tclsh
<Sysname-tcl> system-view
[Sysname-tcl] route-policy 1 permit node 10
[Sysname-tcl-route-policy-1-10] apply cost 10
can't interpret "cost" as a lambda expression
```

2. Configure the **cli** command to execute the Comware command again.

```
[Sysname-tcl-route-policy-1-10] cli apply cost 10
```

Execute multiple Comware commands in one operation.

```
<Sysname> tclsh
<Sysname-tcl> system-view
```

- Method 1:

```
[Sysname-tcl] cli "vlan 2 ; description Tech"
```

- Method 2:

```
[Sysname-tcl] cli vlan 2 ; cli description Tech
```

tclquit

Use **tclquit** to return from Tcl configuration view to user view.

Syntax

tclquit

Views

Tcl configuration view

Predefined user roles

network-admin

Usage guidelines

To return from Tcl configuration view to user view, you can also use the **quit** command.

To return to the upper-level view after you execute Comware commands to enter system view or a Comware feature view, use the **quit** command.

Examples

Return from Tcl configuration view to user view.

```
<Sysname-tcl> tclquit
<Sysname>
```

Related commands

tclsh

tclsh

Use **tclsh** to enter Tcl configuration view from user view.

Syntax

tclsh

Views

User view

Predefined user roles

network-admin

Usage guidelines

In Tcl configuration view, you can execute the following commands:

- All Tcl 8.5 commands.
- Comware commands. The Tcl configuration view is equivalent to the user view. You can use Comware commands in Tcl configuration view in the same way they are used in user view.

Examples

Enter Tcl configuration view from user view.

```
<Sysname> tclsh
<Sysname-tcl>
```

Related commands

tclquit

Contents

Python commands

exit()

Use **exit()** to exit the Python shell.

Syntax

exit()

Views

Python shell

Predefined user roles

network-admin

Usage guidelines

To return to user view from the Python shell, you cannot use the **quit** command. You must use the **exit()** command.

Examples

Exit the Python shell.

```
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>>
>>> exit()
<Sysname>
```

python

Use **python** to enter the Python shell.

Syntax

python

Views

User view

Predefined user roles

network-admin

Usage guidelines

In the Python shell, you can use the following items:

- Python 2.7 commands.
- Python 2.7 standard API.
- Comware 7 extended API.

Examples

Enter the Python shell.

```
<Sysname> python
Python 2.7.3 (default)
```

```
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

python *filename*

Use **python** *filename* to execute a Python script.

Syntax

python *filename* [*param*]

Views

User view

Predefined user roles

network-admin

Parameters

filename: Specifies the name of a Python script on a storage medium of the device. The script name is case sensitive and must use the extension .py. The extension .py is case insensitive.

param: Specifies the parameters to be passed to the script. To enter multiple parameters, use spaces as the delimiter.

Usage guidelines

You cannot perform any operations while you are executing a Python script.

Make sure the statements in the script meet the syntax requirements. The system stops executing a Python script if it finds a statement with syntax errors.

When executing a script, the system uses the defaults for interactive statements. The system does not stop for human input.

Examples

Execute Python script **test.py**.

```
<Sysname> python test.py 1 2
['/flash:/test.py', '1', '2']
```

Contents

License management commands

display license

Use **display license** to display detailed license information.

Syntax

display license [**activation-file**] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

activation-file: Displays license information about activation files.

slot *slot-number*: Specifies the member ID of an IRF member device. If no member device is specified, this command displays license information for all IRF member devices.

Usage guidelines

If you do not specify any parameters, this command displays detailed information about all licenses.

Examples

Display detailed information about all licenses.

```
<Sysname> display license
Slot 1:
flash:/license/210235A1XE012345678920170503175748826 33.ak
Feature: APMGR
Product Description: Enhanced Access Controller License,128 APs,for Verticals,fo
r V7
Registered at: 2013-01-01 09:26:52
License Type: Trial (days restricted)
Trial Time Left (days): 30
Current State: In use
```

Table 1 Command output

Field	Description
Feature	Feature name.
Product Description	License description.
Registered at	Time when the license was installed.
License Type	License type by validity period: • **NA**—The system cannot obtain the license type. • **Permanent**—Purchased license that never expires and is always valid. • **Trial (days restricted)**—Free trial license that is valid for a period of days.
Trial Time Left (days)	Remaining days of the trial period. This field is available for a trial license.

Field	Description

Current State	State of the license:
	• **In use**—The license is being used.
	• **Usable**—The license is available for use.
	  ○ If multiple days-restricted licenses for one feature are installed, only one license is in **In use** state and the rest licenses are in **Usable** state.
	  ○ A date restricted license is in this state if its start date is not reached.
	• **Expired**—The license has expired.
	• **Uninstalled**—The license has been uninstalled.
	• **Unusable**—The license cannot be used.
	• **Invalid**—The license is invalid and cannot be used.

Uninstall Key	This field is available for licenses that have been uninstalled.
Uninstall Date	Date when the activation file was uninstalled.

display license device-id

Use **display license device-id** to display SN and DID information.

Syntax

display license device-id slot *slot-number*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies the member ID of an IRF member device.

Usage guidelines

When you register a license for a device, you must provide its unique SN and DID.

The DID changes each time you use the **license compress** command to compress the license storage. Use the **display license device-id** command to identify the up-to-date DID each time you register licenses.

Examples

Display the SN and DID for the specified slot.

```
<Sysname> display license device-id slot 1
SN: 210235A045B05B0004350
Device ID: flash:/license/210235A045B05B0004350.did
```

display license feature

Use **display license feature** to display brief license information for features.

Syntax

display license feature

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display brief feature license information.

```
<Sysname> display license feature
Slot 1:
Slot 1:
Total: 64  Usage: 0
Feature                         Licensed        State
APMGR                           N               -
```

Table 2 Command output

Field	Description
Total	Total number of licenses that can be installed.
Usage	Number of licenses stored in the license storage.
Feature	Feature that must be licensed before being used.
Licensed	Licensing state of the feature: • **N**—Not licensed. • **Y**—Licensed.
State	License type by purchasing state: • **Formal**—Purchased license. • **Trial**—Trial license. If the feature is not licensed, this field displays a hyphen (-). To use the feature, you must install a valid license for the feature.

license activation-file install

Use **`license activation-file install`** to install an activation file.

Syntax

`license activation-file install` *`file-name`* **`slot`** *`slot-number`*

Views

System view

Predefined user roles

network-admin

Parameters

`file-name`: Specifies the file path, a case-sensitive string of 1 to 127 characters. The activation file must be valid and stored on the device.

`slot` *`slot-number`*: Specifies the member ID of an IRF member device.

Usage guidelines

To install a license activation file successfully, make sure the SN and DID used for registering the feature license matches the current SN and DID of the device.

Activation files are device locked. A licensed feature can run on an IRF member device even after the member device is moved from one IRF fabric to another IRF fabric.

Examples

Install activation file 20130811.ak to the specified slot.

```
<Sysname> system-view
[Sysname] license activation-file install flash:/license/20130811.ak slot 1
This operation might take some time. Do not perform any other operations until the operation
is completed or a failure message is displayed. Please wait...
```

Related commands

display license

display license device-id

license activation-file uninstall

license activation-file uninstall

Use **license activation-file uninstall** to uninstall an activation file.

Syntax

license activation-file uninstall *file-name* **slot** *slot-number*

Views

System view

Predefined user roles

network-admin

Parameters

file-name: Specifies the file path, a case-sensitive string of 1 to 127 characters.

slot *slot-number*: Specifies the member ID of an IRF member device.

Usage guidelines

Use this command to revoke an unexpired license if you want to transfer the license from one device to another.

When an activation file is uninstalled, the system creates an Uninstall file. Use this file together with the SN and DID of the transfer destination to register the license for the transfer destination.

A feature cannot run after you uninstall all of its activation files.

Trial licenses are not transferrable. When you uninstall the activation file of a trial license, no Uninstall file is created.

Examples

Uninstall activation file flash:/license/20130811.ak from the specified slot.

```
<Sysname> system-view
[Sysname] license activation-file uninstall flash:/license/20130811.ak slot 1
This operation might take some time. Do not perform any other operations until the operation
is completed or a failure message is displayed. Please wait...
Uninstall file: flash:/license/20130813.uak
```

Related commands

display license

license activation-file install

license compress

Use **license compress** to compress the license storage.

Syntax

license compress slot *slot-number*

Views

System view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies the member ID of an IRF member device.

Usage guidelines

The license storage is limited. You can execute this command to clear expired licenses and uninstalled licenses from the license storage.

If uninstalled licenses or expired licenses exist on the device, the compression operation will make the DID or DID file change. Before performing a compression, make sure all licenses registered with the old DID or DID file have been installed. You will be unable to install such licenses after the compression.

Examples

Compress the license storage on the specified slot.

```
<Sysname> system-view
[Sysname] license compress slot 1
This command will delete all data relevant to uninstalled and expired keys/licenses,
including Uninstall keys, and create a new device ID for activation keys/files. Make sure
you have saved the Uninstall keys so you can apply for a new activation key/file for the
unexpired licenses that were covered by the uninstalled activation keys/files.
Are you sure you want to continue? [Y/N]: Y

This operation might take some time. Do not perform any other operations until the operation
is completed or a failure message is displayed. Please wait...
```

Virtual Technologies Command Reference

This command reference is applicable to the following switches and software versions:

H3C S5120V2-LI switch series (Release 6308P01 and later)
H3C S3100V3-SI switch series (Release 6309P01 and later)
H3C S5110V2 switch series (Release 6310 and later)
H3C S5110V2-SI switch series (Release 6310 and later)
H3C S5000V3-EI switch series (Release 6310 and later)
H3C S5000V5-EI switch series (Release 6319P01 and later)
H3C S5000E-X switch series (Release 6310 and later)
H3C S5130S-LI switch series (Release 6310 and later)
H3C MS4320V2 switch series (Release 6308P01 and later)
H3C MS4320 switch series (Release 6308P01 and later)
H3C MS4300V2 switch series (Release 6308P01 and later)
H3C MS4200 switch series (Release 6310 and later)
H3C WS5810-WiNet switch series (Release 6308P01 and later)
H3C WS5820-WiNet switch series (Release 6308P01 and later)
H3C WAS6000 switch series (Release 6308P01 and later)
H3C S5000X-EI switch series (Release 6329 and later)
H3C MS4320V3 switch series (Release 6329 and later)
H3C S5120V3-SI switch series (Release 6329 and later)
H3C S5120V3-LI switch series (Release 6329 and later)

New H3C Technologies Co., Ltd.
http://www.h3c.com

Software version: Release 63xx
Document version: 6W105-20230524

Preface

This command reference describes IRF configuration commands for setting up and maintaining an IRF fabric, including:

This preface includes the following topics about the documentation:

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Documentation feedback

You can e-mail your comments about product documentation to info@h3c.com.

We appreciate your comments.

Contents

IRF commands

display irf

Use **display irf** to display IRF fabric information.

Syntax

display irf

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display IRF fabric information.

```
<Sysname> display irf
MemberID   Role     Priority    CPU-Mac           Description
   1       Loading  1           00e0-fcbe-3102    F1Num001
 *+2       Master   1           00e0-fcb1-ade2    F1Num002
-------------------------------------------------------------

 * indicates the device is the master.
 + indicates the device through which the user logs in.

 The Bridge MAC of the IRF is: 00e0-fc00-1000
 Auto upgrade                  : yes
 Mac persistent                : always
 Domain ID                     : 30
```

Table 1 Command output

Field	Description
MemberID	IRF member ID: • ID of the master is prefixed with an asterisk (*) sign. • ID of the device where you are logged in is prefixed with a plus (+) sign.
Role	Role of the member device in the IRF fabric: • **Standby**—Subordinate device. • **Master**—Master device. • **Loading**—The device is loading software images.
Priority	IRF member priority.
CPU-MAC	MAC address of the CPU in the device.

Field	Description
Description	Description you have configured for the member device. • If no description is configured, this field displays a dashed line (-----). • If the description exceeds the maximum number of characters that can be displayed, an ellipsis (…) is displayed in place of the exceeding text. To display the complete description, use the **display current-configuration** command.
Auto upgrade	Status of the software auto-update feature: • **yes**—Enabled. • **no**—Disabled.
MAC persistent	IRF bridge MAC persistence setting: • **6 min**—Bridge MAC address of the IRF fabric remains unchanged for 6 minutes after the address owner leaves. • **always**—Bridge MAC address of the IRF fabric does not change after the address owner leaves. • **no**—Bridge MAC address of the current master replaces the original bridge MAC address as soon as the owner of the original address leaves.
Domain ID	Domain ID of the IRF fabric. The domain ID you assign to an IRF fabric must uniquely identify the fabric in a multi-IRF fabric network.

Related commands

display irf configuration

display irf topology

display irf configuration

Use **display irf configuration** to display basic IRF settings for each member device.

Syntax

display irf configuration

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display basic IRF settings for all members.

```
<Sysname> display irf configuration
 MemberID  NewID    IRF-Port1                  IRF-Port2
 1         1        Ten-GigabitEthernet1/0/49  Ten-GigabitEthernet1/0/51
 2         2        Ten-GigabitEthernet2/0/49  Ten-GigabitEthernet2/0/51
                    Ten-GigabitEthernet2/0/50
 4         4        Ten-GigabitEthernet4/0/49  Ten-GigabitEthernet4/0/51
                                               Ten-GigabitEthernet4/0/52
```

Table 2 Command output

Field	Description
MemberID	Current member ID of the device.
NewID	Member ID assigned to the device. This member ID takes effect at reboot.
IRF-Port1	Physical interfaces bound to IRF-port 1. This field displays **disable** if no physical interfaces are bound to the IRF port.
IRF-Port2	Physical interfaces bound to IRF-port 2. This field displays **disable** if no physical interfaces are bound to the IRF port.

Related commands

`display irf`

`display irf topology`

display irf link

Use **`display irf link`** to display IRF link information.

Syntax

`display irf link`

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display IRF link information.

```
<Sysname> display irf link
Member 1
 IRF Port    Interface                      Status
 1           disable                        --
 2           Ten-GigabitEthernet1/0/51      UP
             Ten-GigabitEthernet1/0/52      ADM
Member 2
 IRF Port    Interface                      Status
 1           Ten-GigabitEthernet2/0/51      UP
             Ten-GigabitEthernet2/0/52      DOWN
 2           disable                        --
```

Table 3 Command output

Field	Description
Member *ID*	IRF member ID.
IRF Port	IRF port number: • **1**—IRF-port 1. • **2**—IRF-port 2.

Field	Description
Interface	Physical interfaces bound to the IRF port. This field displays **disable** if no physical interfaces have been bound to the IRF port.
Status	Link state of the IRF physical interface: • **UP**—The link is up. • **DOWN**—The link is down. • **ADM**—The interface has been manually shut down by using the **shutdown** command.

display irf topology

Use **display irf topology** to display IRF fabric topology information.

Syntax

display irf topology

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the IRF fabric topology.

```
<Sysname> display irf topology
                          Topology Info
 ------------------------------------------------------------------------
              IRF-Port1                 IRF-Port2
 MemberID   Link        neighbor      Link        neighbor     Belong To
 1          DOWN        ---           UP          2            000f-cbb8-1a82
 2          UP          1             DIS         ---          000f-cbb8-1a82
```

Table 4 Command output

Field	Description
IRF-Port1	Information about IRF-port 1, including its link state and neighbor.
IRF-Port2	Information about IRF-port 2, including its link state and neighbor.
MemberID	IRF member ID.

Field	Description

Link	Link state of the IRF port:
	• **UP**—The IRF link is up.
	• **DOWN**—The IRF link is down because the port has no physical link or has not been activated by the **irf-port-configuration active** command.
	• **DIS**—No physical interfaces have been bound to the IRF port.
	• **TIMEOUT**—IRF hello interval has timed out.
	• **ISOLATE**—The device is isolated from the IRF fabric. This issue might be caused by the following reasons:
	  ○ The IRF fabric does not support the device model.
	  ○ The maximum number of member devices has exceeded the upper limit.

neighbor	IRF member ID of the device connected to the IRF port. This field displays three hyphens (---) if no device is connected to the port.
Belong To	IRF fabric that has the device, represented by the CPU MAC address of the master in the IRF fabric.

Related commands

display irf

display irf configuration

display mad

Use **display mad** to display MAD status and settings.

Syntax

display mad [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

verbose: Displays detailed MAD information. If you do not specify this keyword, the command only displays whether a MAD mechanism is enabled or disabled.

Examples

Display brief MAD information.

```
<Sysname> display mad
MAD ARP disabled.
MAD ND disabled.
MAD LACP enabled.
MAD BFD enabled.
```

Display detailed MAD information.

```
<Sysname> display mad verbose
Multi-active recovery state: No
```

```
Excluded ports (user-configured):
  Bridge-Aggregation4
  Vlan-interface999
Excluded ports (system-configured):
  IRF physical interfaces:
    Ten-GigabitEthernet1/0/51
    Ten-GigabitEthernet1/0/52
    Ten-GigabitEthernet2/0/51
    Ten-GigabitEthernet2/0/52
  BFD MAD interfaces:
    GigabitEthernet1/0/10
    GigabitEthernet2/0/10
    Vlan-interface3
  Member interfaces of excluded interface Bridge-Aggregation 4:
    GigabitEthernet1/0/11
    GigabitEthernet2/0/11
MAD ARP disabled.
MAD ND disabled.
MAD LACP enabled interface: Bridge-Aggregation 1
  MAD status                 : Normal
  Member ID       Port                       MAD status
  1               GigabitEthernet1/0/1       Normal
  2               GigabitEthernet2/0/1       Normal
MAD BFD enabled interface: VLAN-interface 3
  MAD status                 : Normal
  Member ID   MAD IP address       Neighbor    MAD status
  1           192.168.1.1/24       2           Normal
  2           192.168.1.2/24       1           Normal
```

Table 5 Command output

Field	Description
MAD ARP disabled.	Status of ARP MAD. This field displays **MAD ARP enabled** if ARP MAD is enabled.
MAD ND disabled.	Status of ND MAD. This field displays **MAD ND enabled** if ND MAD is enabled.
MAD LACP enabled.	Status of LACP MAD. This field displays **MAD LACP disabled** if LACP MAD is disabled.
MAD BFD enabled.	Status of BFD MAD. This field displays **MAD BFD disabled** if BFD MAD is disabled.
Multi-active recovery state	Whether the IRF fabric is in Recovery state: • **Yes**—The IRF fabric is in Recovery state. When MAD detects that an IRF fabric has split into multiple IRF fabrics, it allows one fabric to forward traffic. All the other IRF fabrics are set to the Recovery state. In Recovery state, MAD shuts down all common network interfaces in the fabric except for the system- and user-excluded network interfaces. • **No**—The IRF fabric is not in Recovery state. It is active and can forward traffic.

Field	Description
Excluded ports (user-configured)	Network interfaces manually configured to not shut down when the IRF fabric transits to the Recovery state.

Excluded ports (system-configured)	Network interfaces set to not shut down by the system when the IRF fabric transits to the Recovery state. These interfaces are not manually configured.
	• IRF physical interfaces.
	• BFD MAD interfaces:
	  ○ VLAN interfaces used for BFD MAD and the Layer 2 Ethernet ports in the VLANs.
	  ○ Management Ethernet ports used for BFD MAD.
	• Member interfaces of a Layer 2 aggregate interface if the aggregate interface is excluded from the MAD shutdown action.

MAD ARP enabled interface:	Interfaces on which ARP MAD is enabled. This field displays **MAD ARP disabled** if ARP MAD is disabled.
MAD ND enabled interface:	Interfaces on which ND MAD is enabled. This field displays **MAD ND disabled** if ND MAD is disabled.
MAD LACP enabled interface	Interface on which LACP MAD is enabled. This field is displayed for each interface enabled with LACP MAD. This field displays **MAD LACP disabled** if LACP MAD is disabled.

MAD status	LACP MAD operating status:
	• **Normal**—LACP MAD is operating correctly.
	• **Faulty**—LACP MAD is not operating correctly. Verify the following items:
	  ○ Verify that the ports on LACP MAD links are up.
	  ○ Verify that the intermediate device supports extended LACPDUs.
	  ○ Verify that all member devices have member ports used for LACP MAD.

Member ID Port MAD status	LACP MAD details: • **Member ID**—IRF member ID of a device. • **Port**—Member ports of the aggregate interface used for LACP MAD. • **MAD status**—LACP MAD operating state on a member port. Values include **Normal** and **Faulty**.
MAD BFD enabled interface:	Layer 3 interface on which BFD MAD is enabled. This field displays **MAD BFD disabled** if BFD MAD is disabled.
MAD status	BFD MAD operating status: • **Normal**—BFD MAD is operating correctly. • **Faulty**—BFD MAD is not operating correctly. Check the BFD MAD link for connectivity issues. • **N/A**—BFD MAD link status cannot be detected. If BFD MAD is enabled on a management Ethernet port, it is normal that this field displays **N/A**.

Member ID
MAD IP address
Neighbor
MAD status
	BFD MAD details:
	• **Member ID**—IRF member ID of the local device.
	• **MAD IP address**—MAD IP address of a member device.
	• **Neighbor**—IRF member ID of the neighboring member device.
	• **MAD status**—BFD MAD link state. The following values are available:
	  ○ **Normal**—BFD MAD is operating correctly.
	  ○ **Faulty**—BFD MAD is not operating correctly. Check the BFD MAD link for connectivity issues.
	  ○ **N/A**—BFD MAD link status cannot be detected. If BFD MAD is enabled on a management Ethernet port, it is normal that this field displays **N/A**.

easy-irf

Use **easy-irf** to bulk-configure basic IRF settings for an IRF member device.

Syntax

easy-irf [**member** *member-id* [**renumber** *new-member-id*] **domain** *domain-id* [**priority** *priority*] [**irf-port1** *interface-list1*] [**irf-port2** *interface-list2*]]

Views

System view

Predefined user roles

network-admin

Parameters

member *member-id*: Specifies the member ID of a member device. The value range for the member ID is 1 to 10.

renumber *new-member-id*: Specifies a new member ID for the device. The value range for the member ID is 1 to 10. The member device automatically reboots for the new member ID to take effect. If you do not specify this option, the command does not change the member ID.

domain *domain-id*: Specifies an IRF domain ID in the range of 0 to 4294967295. Assign the same domain ID to all devices you are adding to the same IRF fabric.

priority *priority*: Specifies an IRF priority in the range of 1 to 32. The greater the priority value, the higher the priority. A member with higher priority is more likely to be the master.

irf-port1 *interface-list1*: Specifies interfaces bound to IRF-port 1. The *interface-list1* argument represents a space-separated list of up to eight interface items. Each interface item specifies one interface in the *interface-type interface-number* form.

irf-port2 *interface-list2*: Specifies interfaces bound to IRF-port 2. A physical interface can be bound to only one IRF port. The *interface-list2* argument represents a space-separated list of up to eight interface items. Each interface item specifies one interface in the *interface-type interface-number* form.

Usage guidelines

This command bulk-configures basic IRF settings for a member device, including the member ID, domain ID, priority, and IRF port bindings.

The easy IRF feature provides the following configuration methods:

- **Interactive method**—Enter the **easy-irf** command without parameters. The system will guide you to set the parameters step by step.
- **Non-interactive method**—Enter the **easy-irf** command with parameters.

As a best practice, use the interactive method if you are new to IRF.

If you execute this command multiple times, the following settings take effect:

- The most recent settings for the member ID, domain ID, and priority.
- IRF port bindings added through repeated executions of the command.

The software supports binding a maximum of eight physical interfaces to an IRF port. However, you might be unable to bind as many as eight physical interfaces to an IRF port due to hardware restrictions.

When you specify physical interfaces for an IRF port, you must follow the IRF port binding requirements in *Virtual Technologies Configuration Guide*.

If you specify physical interfaces by using the interactive method, you must also follow these restrictions and guidelines:

- Do not enter spaces between the interface type and interface number.
- Use a comma (,) to separate two physical interfaces. No spaces are allowed between interfaces.

To remove an IRF physical interface from an IRF port, you must use the **undo port group interface** command in IRF port view.

Examples

Bulk-configure basic IRF settings by using the non-interactive method. Change the member ID from 2 to 3, set the domain ID to 10, configure the member priority as 10, and bind Ten-GigabitEthernet 2/0/51 and Ten-GigabitEthernet 2/0/52 to IRF-port 1.

```
<Sysname> system-view
[Sysname] easy-irf member 2 renumber 3 domain 10 priority 10 irf-port1 ten-gigabitethernet
2/0/51 ten-gigabitethernet 2/0/52
*************************************************************************
                  Configuration summary for member 2
IRF new member ID: 3
IRF domain ID    : 10
IRF priority     : 10
IRF-port 1       : Ten-GigabitEthernet2/0/51, Ten-GigabitEthernet2/0/52
IRF-port 2       : Disabled
*************************************************************************
Are you sure to use these settings to set up IRF? [Y/N] y
Starting to configure IRF...
Configuration succeeded.
The device will reboot for the new member ID to take effect. Continue? [Y/N] y
```

Bulk-configure basic IRF settings by using the interactive method. Change the member ID from 2 to 3, set the domain ID to 10, configure the member priority as 10, and bind Ten-GigabitEthernet 2/0/51 and Ten-GigabitEthernet 2/0/52 to IRF-port 1.

```
<Sysname> system-view
[Sysname] easy-irf
*************************************************************************
Welcome to use easy IRF.
To skip the current step, enter a dot sign (.).
To return to the previous step, enter a minus sign (-).
To use the default value (enclosed in []) for each parameter, press Enter without
entering a value.
To quit the setup procedure, press CTRL+C.
*************************************************************************
Select a member by its ID <2> [2]:2
Specify a new member ID <1~10> [1]: 3
Specify a domain ID <0~4294967295> [0]: 10
Specify a priority <1~32> [1]: 10
Specify IRF-port 1 bindings (a physical interface or a comma-separated physical
interface list)[Disabled]: ten-gigabitethernet2/0/51,ten-gigabitethernet2/0/52
Specify IRF-port 2 bindings (a physical interface or a comma-separated physical
interface list)[Disabled]:
*************************************************************************
```

```
                  Configuration summary for member 2
IRF new member ID: 3
IRF domain ID    : 10
IRF priority     : 10
IRF-port 1       : Ten-GigabitEthernet2/0/51, Ten-GigabitEthernet2/0/52
IRF-port 2       : Disabled
*************************************************************************
Are you sure to use these settings to set up IRF? [Y/N] y
Starting to configure IRF...
Configuration succeeded.
The device will reboot for the new member ID to take effect. Continue? [Y/N] y
```

irf auto-update enable

Use **irf auto-update enable** to enable the software auto-update feature.

Use **undo irf auto-update enable** to disable the software auto-update feature.

Syntax

irf auto-update enable

undo irf auto-update enable

Default

Software auto-update is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command automatically propagates the current software images of the master device in the IRF fabric to any devices you are adding to the IRF fabric.

To ensure a successful software update, verify that the new device you are adding to the IRF fabric has sufficient storage space for the new software images. If sufficient storage space is not available, the device automatically deletes the current software images. If the reclaimed space is still insufficient, the device cannot complete the auto-update. You must reboot the device, and then access the BootWare menu to delete files.

Examples

Enable the software auto-update feature.

```
<Sysname> system-view
[Sysname] irf auto-update enable
```

irf domain

Use **irf domain** to assign a domain ID to the IRF fabric.

Use **undo irf domain** to restore the default.

Syntax

irf domain *domain-id*

undo irf domain

Default

The IRF domain ID is 0.

Views

System view

Predefined user roles

network-admin

Parameters

domain-id: Specifies a domain ID for the IRF fabric. The value range is 0 to 4294967295.

Usage guidelines

CAUTION:

Changing the IRF domain ID of an IRF member device will remove that member device from the IRF fabric. This member device will be unable to exchange IRF protocol packets with the remaining member devices in the IRF fabric.

One IRF fabric forms one IRF domain. IRF uses IRF domain IDs to uniquely identify IRF fabrics and prevent IRF fabrics from interfering with one another.

If one IRF fabric uses another IRF fabric as the intermediate device for LACP MAD, ARP MAD, or ND MAD, you must assign the two IRF fabrics different domain IDs for correct split detection. False detection causes IRF split.

An IRF fabric has only one IRF domain ID. You can change the IRF domain ID by using the following commands: **irf domain**, **mad enable**, **mad arp enable**, or **mad nd enable**. The IRF domain IDs configured by using these commands overwrite each other.

Examples

Set the IRF domain ID to 10.

```
<Sysname> system-view
[Sysname] irf domain 10
```

irf link-delay

Use **irf link-delay** to set a delay for the IRF ports to report a link status change event.

Use **undo irf link-delay** to restore the default.

Syntax

irf link-delay *interval*

undo irf link-delay

Default

The delay time is 4 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Sets the IRF link status change report delay, in the range of 0 to 10000 milliseconds. If the interval is set to 0, link status change events are reported without any delay.

Usage guidelines

The device delays reporting link status change events of an IRF port, but it does not delay reporting link status change events of an IRF physical interface.

Examples

Set the IRF link status change report delay to 300 milliseconds.

```
<Sysname> system-view
[Sysname] irf link-delay 300
```

irf mac-address persistent

Use **irf mac-address persistent** to configure IRF bridge MAC persistence.

Use **undo irf mac-address persistent** to disable IRF bridge MAC persistence.

Syntax

irf mac-address persistent { **always** | **timer** }

undo irf mac-address persistent

Default

The IRF bridge MAC address remains unchanged for 6 minutes after the address owner leaves.

Views

System view

Predefined user roles

network-admin

Parameters

always: Enables the IRF bridge MAC address to be permanent. The IRF bridge MAC address does not change after the address owner leaves the fabric.

timer: Enables the IRF bridge MAC address to remain unchanged for 6 minutes after the address owner leaves. If the owner rejoins the IRF fabric within the time limit, the IRF bridge MAC address does not change. If the owner does not rejoin the IRF fabric within the time limit, the IRF fabric uses the bridge MAC address of the current master as the bridge MAC address.

Usage guidelines

CAUTION:

IRF bridge MAC address change will cause transient traffic disruption.

If the **undo** form of this command is used, bridge MAC address of the current master replaces the original IRF bridge MAC as soon as the original address owner leaves.

If ARP MAD or ND MAD is used with the spanning tree feature, disable IRF bridge MAC persistence by using the **undo irf mac-address persistent** command.

If the IRF fabric uses a daisy-chain topology and has aggregate links with upstream or downstream devices, do not execute the **undo irf mac-address persistent** command. Use of this command might result in transmission delay or packet loss after the address owner leaves or reboots.

If the IRF fabric has multichassis aggregate links, do not use the **undo irf mac-address persistent** command. Use of this command might cause traffic disruption.

By default, an IRF fabric uses the bridge MAC address of the master device as its bridge MAC address.

On a switched LAN, the IRF bridge MAC address must be unique for correct traffic transmission.

When IRF fabrics merge, IRF ignores the IRF bridge MAC address and checks the bridge MAC address of each member device in the IRF fabrics. IRF merge fails if any two member devices have the same bridge MAC address.

Examples

Enable the IRF bridge MAC address to persist forever.

```
<Sysname> system-view
[Sysname] irf mac-address persistent always
```

irf member description

Use **irf member description** to configure a description for an IRF member device.

Use **undo irf member description** to restore the default.

Syntax

irf member *member-id* **description** *text*

undo irf member *member-id* **description**

Default

No description is configured for an IRF member device.

Views

System view

Predefined user roles

network-admin

Parameters

member-id: Specifies the ID of an IRF member.

text: Specifies a description, a string of 1 to 127 characters.

Examples

Configure the description as **F1Num001** for IRF member 1.

```
<Sysname> system-view
[Sysname] irf member 1 description F1Num001
```

irf member priority

Use **irf member priority** to change the priority of an IRF member device.

Use **undo irf member priority** to restore the default.

Syntax

irf member *member-id* **priority** *priority*

undo irf member *member-id* **priority**

Default

The IRF member priority is 1.

Views

System view

Predefined user roles

network-admin

Parameters

member-id: Specifies an IRF member ID. The value range for IRF member IDs is 1 to 10.

priority: Sets priority in the range of 1 to 32. The greater the priority value, the higher the priority. A member with higher priority is more likely to be the master.

Usage guidelines

The new priority setting takes effect at the next master election, but it does not trigger a master election.

Examples

Set the priority of IRF member 2 to 32.

```
<Sysname> system-view
[Sysname] irf member 2 priority 32
```

irf member renumber

Use **irf member renumber** to change the member ID of an IRF member device.

Use **undo irf member renumber** to restore the previous IRF member ID of the device.

Syntax

irf member *member-id* **renumber** *new-member-id*

undo irf member *member-id* **renumber**

Default

The IRF member ID is 1.

Views

System view

Predefined user roles

network-admin

Parameters

member-id: Specifies the ID of an IRF member. The value range for IRF member IDs is 1 to 10.

new-member-id: Assigns a new ID to the IRF member. The value range for IRF member IDs is 1 to 10.

Usage guidelines

CAUTION:

IRF member ID change can invalidate member ID-related settings, including interface and file path settings, and cause data loss. Make sure you fully understand its impact on your live network.

To have the new ID take effect, you must reboot the IRF member. To cancel the member ID change before you reboot the member device, use the **undo irf member renumber** command. In the command, set the new member ID to be the same as the old member ID.

When adding a device into an IRF fabric, you must assign a unique IRF member ID to the device. If its IRF member ID has been used in the IRF fabric, the device cannot join the IRF fabric.

Interchanging member IDs between IRF member devices might cause undesirable configuration changes and data loss. For example, the IRF member IDs of Device A and Device B are 2 and 3, respectively. After you interchange their member IDs, their port settings also interchange.

Examples

Change the ID of an IRF member device from 1 to 2.

```
<Sysname> display irf
[Sysname] irf member 1 renumber 2
Renumbering the member ID may result in configuration change or loss. Continue?[Y/N]Y
```

Before rebooting the device, cancel the change in the preceding example.

```
[Sysname] undo irf member 1 renumber
Renumbering the member ID may result in configuration change or loss. Continue?[Y/N]y
```

If you reboot the device after executing the **irf member 1 renumber 2** command, the device member ID changes to 2 at system reboot. Using **undo irf member 1 renumber** cannot restore the member ID to 1. You must use the **irf member 2 renumber 1** command to reconfigure the member ID.

irf-port

Use **irf-port** to enter IRF port view.

Use **undo irf-port** to remove all port bindings on an IRF port.

Syntax

irf-port *member-id/irf-port-number*

undo irf-port *member-id/irf-port-number*

Views

System view

Predefined user roles

network-admin

Parameters

member-id: Specifies an IRF member device by its member ID.

irf-port-number: Specifies an IRF port on the member device. The *irf-port-number* argument represents the IRF port index and must be 1 or 2.

Usage guidelines

To bind physical interfaces to an IRF port, you must enter IRF port view.

Examples

Enter IRF-port 2/1 view.

```
<Sysname> system-view
[Sysname] irf-port 2/1
[Sysname-irf-port2/1]
```

Related commands

`port group interface`

irf-port-configuration active

Use **`irf-port-configuration active`** to activate IRF ports.

Syntax

`irf-port-configuration active`

Views

System view

Predefined user roles

network-admin

Usage guidelines

After connecting the physical interfaces between two devices and binding them to the correct IRF ports, you must use this command to activate the settings on the IRF ports. This command merges the two devices into one IRF fabric.

The system activates the IRF port settings automatically in the following situations:

- The configuration file that the device starts with contains IRF port bindings.
- You are binding physical interfaces to an IRF port after an IRF fabric is formed.

Examples

To configure and activate IRF-port 1/2 when the port is in DIS state:

Bind Ten-GigabitEthernet 1/0/51 to IRF-port 1/2.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/51
[Sysname-Ten-GigabitEthernet1/0/51] shutdown
[Sysname-Ten-GigabitEthernet1/0/51] quit
[Sysname] irf-port 1/2
[Sysname-irf-port1/2] port group interface ten-gigabitethernet 1/0/51
You must perform the following tasks for a successful IRF setup:
Save the configuration after completing IRF configuration.
Execute the "irf-port-configuration active" command to activate the IRF ports.
[Sysname-irf-port1/2] quit
[Sysname] interface ten-gigabitethernet 1/0/51
[Sysname-Ten-GigabitEthernet1/0/51] undo shutdown
[Sysname-Ten-GigabitEthernet1/0/51] quit
```

Save the configuration so the IRF port settings can take effect after the device reboots.

```
[Sysname] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait.........................
Saved the current configuration to mainboard device successfully.
```

Activate the IRF port.

```
[Sysname] irf-port-configuration active
```

mad arp enable

Use **mad arp enable** to enable ARP MAD.

Use **undo mad arp enable** to disable ARP MAD.

Syntax

mad arp enable

undo mad arp enable

Default

ARP MAD is disabled.

Views

Management Ethernet interface view

VLAN interface view

Predefined user roles

network-admin

Usage guidelines

Do not configure ARP MAD together with LACP MAD or BFD MAD, because they handle collisions differently.

When you configure ARP MAD on a VLAN interface, follow these restrictions and guidelines:

Category	Restrictions and guidelines

ARP MAD VLAN	• Do not enable ARP MAD on VLAN-interface 1.
	• If you are using an intermediate device, perform the following tasks:
	  ○ On the IRF fabric and the intermediate device, create a VLAN for ARP MAD.
	  ○ On the IRF fabric and the intermediate device, assign the ports of ARP MAD links to the ARP MAD VLAN.
	  ○ On the IRF fabric, create a VLAN interface for the ARP MAD VLAN.
	• As a best practice, do not use the ARP MAD VLAN for any other purposes.

ARP MAD and feature configuration	If an intermediate device is used, make sure the following requirements are met: • Run the spanning tree feature between the IRF fabric and the intermediate device to ensure that there is only one ARP MAD link in forwarding state. For more information about the spanning tree feature and its configuration, see *Layer 2—LAN Switching Configuration Guide*. • Enable the IRF fabric to change its bridge MAC address as soon as the address owner leaves. • If the intermediate device is also an IRF fabric, assign the two IRF fabrics different domain IDs for correct split detection.

When you configure ARP MAD on a management Ethernet port, follow these restrictions and guidelines:

Category	Restrictions and guidelines
Management Ethernet ports for ARP MAD	Connect a management Ethernet port on each member device to the common Ethernet ports on the intermediate device.

Category	Restrictions and guidelines
ARP MAD VLAN	On the intermediate device, create a VLAN for ARP MAD, and assign the ports used for ARP MAD to the VLAN. On the IRF fabric, you do not need to assign the management Ethernet ports to the VLAN.
ARP MAD and feature configuration	• Enable the IRF fabric to change its bridge MAC address as soon as the address owner leaves. • If the intermediate device is also an IRF fabric, assign the two IRF fabrics different domain IDs for correct split detection.

When you use the **mad arp enable** command, the system prompts you to enter a domain ID. If you do not want to change the current domain ID, press **enter** at the prompt.

An IRF fabric has only one IRF domain ID. You can change the IRF domain ID by using the following commands: **irf domain**, **mad enable**, **mad arp enable**, or **mad nd enable**. The IRF domain IDs configured by using these commands overwrite each other.

Examples

Enable ARP MAD on VLAN-interface 3.

```
<Sysname> system-view
[Sysname] interface vlan-interface 3
[Sysname-Vlan-interface3] mad arp enable
You need to assign a domain ID (range: 0-4294967295)
[Current domain is: 0]: 1
The assigned domain ID is: 1
```

Related commands

irf domain

mad bfd enable

Use **mad bfd enable** to enable BFD MAD.

Use **undo mad bfd enable** to disable BFD MAD.

Syntax

mad bfd enable

undo mad bfd enable

Default

BFD MAD is disabled.

Views

VLAN interface view

Management Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

Do not configure BFD MAD together with ARP MAD or ND MAD, because they handle collisions differently.

When you configure BFD MAD on a VLAN interface, follow these guidelines:

Category	Restrictions and guidelines

BFD MAD VLAN	• Do not enable BFD MAD on VLAN-interface 1.
	• If you are using an intermediate device, perform the following tasks:
	  ○ On the IRF fabric and the intermediate device, create a VLAN for BFD MAD.
	  ○ On the IRF fabric and the intermediate device, assign the ports of BFD MAD links to the BFD MAD VLAN.
	  ○ On the IRF fabric, create a VLAN interface for the BFD MAD VLAN.
	• Make sure the IRF fabrics on the network use different BFD MAD VLANs.
	• Make sure the BFD MAD VLAN contains only ports on the BFD MAD links. Exclude a port from the BFD MAD VLAN if that port is not on a BFD MAD link. If you have assigned that port to all VLANs by using the **`port trunk permit vlan all`** command, use the **`undo port trunk permit`** command to exclude that port from the BFD MAD VLAN.

BFD MAD VLAN and feature compatibility	Do not use the BFD MAD VLAN for any purposes other than configuring BFD MAD. • Use only the **`mad bfd enable`** and **`mad ip address`** commands on the BFD MAD-enabled VLAN interface. If you configure other features, both BFD MAD and other features on the interface might run incorrectly. • Disable the spanning tree feature on any Layer 2 Ethernet ports in the BFD MAD VLAN. The MAD feature is mutually exclusive with the spanning tree feature.
MAD IP address	• To avoid network issues, only use the **`mad ip address`** command to configure IP addresses on the BFD MAD-enabled VLAN interface. Do not configure an IP address by using the **`ip address`** command on the BFD MAD-enabled VLAN interface. • Make sure all the MAD IP addresses are on the same subnet.

When you configure BFD MAD on a management Ethernet port, follow these restrictions and guidelines:

Category	Restrictions and guidelines
Management Ethernet ports for BFD MAD	Connect a management Ethernet port on each member device to the common Ethernet ports on the intermediate device.
BFD MAD VLAN	• On the intermediate device, create a VLAN for BFD MAD, and assign the ports used for BFD MAD to the VLAN. On the IRF fabric, you do not need to assign the management Ethernet ports to the VLAN. • Make sure the IRF fabrics on the network use different BFD MAD VLANs. • Make sure the BFD MAD VLAN on the intermediate device contains only ports on the BFD MAD links.
MAD IP address	• Use the **`mad ip address`** command instead of the **`ip address`** command to configure MAD IP addresses on the BFD MAD-enabled management Ethernet ports. • Make sure all the MAD IP addresses are on the same subnet.

Examples

Enable BFD MAD on VLAN-interface 3.

```
<Sysname> system-view
[Sysname] interface vlan-interface 3
[Sysname-Vlan-interface3] mad bfd enable
```

mad enable

Use **mad enable** to enable LACP MAD.

Use **undo mad enable** to disable LACP MAD.

Syntax

mad enable

undo mad enable

Default

LACP MAD is disabled.

Views

Aggregate interface view

Predefined user roles

network-admin

Usage guidelines

LACP MAD handles collisions differently than ARP MAD and ND MAD. To avoid conflicts, do not enable LACP MAD together with ARP MAD and ND MAD on an IRF fabric.

LACP MAD requires a device that supports extended LACPDUs for MAD to act as the intermediate device. You must set up a dynamic link aggregation group that spans all IRF member devices between the IRF fabric and the intermediate device. To enable dynamic link aggregation, configure the **link-aggregation mode dynamic** command on the aggregate interface.

If one IRF fabric uses another IRF fabric as the intermediate device for LACP MAD, you must assign the two IRF fabrics different domain IDs for correct split detection. False detection causes IRF split.

When you use the **mad enable** command, the system prompts you to enter a domain ID. If you do not want to change the current domain ID, press **enter** at the prompt.

An IRF fabric has only one IRF domain ID. You can change the IRF domain ID by using the following commands: **irf domain**, **mad enable**, **mad arp enable**, or **mad nd enable**. The IRF domain IDs configured by using these commands overwrite each other.

Examples

Enable LACP MAD on Bridge-Aggregation 1, a Layer 2 dynamic aggregate interface.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] link-aggregation mode dynamic
[Sysname-Bridge-Aggregation1] mad enable
You need to assign a domain ID (range: 0-4294967295)
[Current domain ID is: 0]: 1
The assigned domain ID is: 1
```

Related commands

irf domain

mad exclude interface

Use **mad exclude interface** to exclude an interface from being shut down when the IRF fabric transits to the Recovery state upon detection of a multi-active collision.

Use **undo mad exclude interface** to configure the IRF fabric to shut down an interface when it transits to the Recovery state upon detection of a multi-active collision.

Syntax

mad exclude interface *interface-type interface-number*

undo mad exclude interface *interface-type interface-number*

Default

Except for the network interfaces automatically excluded by the system, all network interfaces are shut down when the IRF fabric transits to the Recovery state. The system automatically excludes the following network interfaces from being shut down:

- IRF physical interfaces.
- Interfaces used for BFD MAD.
- Member interfaces of an aggregate interface if the aggregate interface is excluded from being shut down.

Views

System view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

If an interface must be kept in up state for special purposes such as Telnet connection, exclude the interface from the shutdown action. As a best practice to avoid incorrect traffic forwarding, do not exclude any interfaces except the interfaces used for Telnet.

The interfaces that have been shut down by MAD come up when the member devices reboot to join the recovered IRF fabric. If the active IRF fabric fails before the IRF link is recovered, use the **mad restore** command on the inactive IRF fabric to recover the inactive IRF fabric. This command also brings up all interfaces that were shut down by MAD.

Examples

Exclude GigabitEthernet 1/0/1 from being shut down when the MAD status transits to Recovery.

```
<Sysname> system-view
[Sysname] mad exclude interface gigabitethernet 1/0/1
```

Related commands

mad restore

mad ip address

Use **mad ip address** to assign a MAD IP address to an IRF member device for BFD MAD.

Use **undo mad ip address** to delete the MAD IP address for an IRF member device.

Syntax

mad ip address *ip-address* { *mask* | *mask-length* } **member** *member-id*

undo mad ip address *ip-address* { *mask* | *mask-length* } **member** *member-id*

Default

No MAD IP address is configured for an IRF member device.

Views

VLAN interface view

Management Ethernet interface view

Predefined user roles

network-admin

Parameters

ip-address: Specifies an IP address in dotted decimal notation.

mask: Specifies a subnet mask in decimal dotted notation.

mask-length: Specifies a subnet mask in length, in the range of 0 to 32.

member *member-id*: Specifies the ID of an IRF member.

Usage guidelines

To use BFD MAD, configure a MAD IP address for each IRF member. Make sure all the MAD IP addresses are on the same subnet.

Do not configure a MAD IP address by using the **ip address** command on the BFD MAD-enabled port or interface.

The master attempts to establish BFD sessions with other member devices by using its MAD IP address as the source IP address.

- If the IRF fabric is integrated, only the MAD IP address of the master takes effect. The master cannot establish a BFD session with any other member. If you execute the **display bfd session** command, the state of the BFD sessions is **Down**.
- When the IRF fabric splits, the IP addresses of the masters in the partitioned IRF fabrics take effect. The masters can establish a BFD session. If you execute the **display bfd session** command, the state of the BFD session between the two devices is **Up**.

Examples

Assign a MAD IP address to IRF member 1 on VLAN-interface 3.

```
<Sysname> system-view
[Sysname] interface vlan-interface 3
[Sysname-Vlan-interface3] mad ip address 192.168.0.1 255.255.255.0 member 1
```

Assign a MAD IP address to IRF member 2 on VLAN-interface 3.

```
[Sysname-Vlan-interface3] mad ip address 192.168.0.2 255.255.255.0 member 2
```

Related commands

mad bfd enable

mad nd enable

Use **mad nd enable** to enable ND MAD.

Use **undo mad nd enable** to disable ND MAD.

Syntax

mad nd enable

undo mad nd enable

Default

ND MAD is disabled.

Views

VLAN interface view

Management Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

Do not configure ND MAD together with LACP MAD or BFD MAD, because they handle collisions differently.

When you configure ND MAD on a VLAN interface, follow these restrictions and guidelines:

Category	Restrictions and guidelines

ND MAD VLAN	• Do not enable ND MAD on VLAN-interface 1.
	• If you are using an intermediate device, perform the following tasks:
	  ○ On the IRF fabric and the intermediate device, create a VLAN for ND MAD.
	  ○ On the IRF fabric and the intermediate device, assign the ports of ND MAD links to the ND MAD VLAN.
	  ○ On the IRF fabric, create a VLAN interface for the ND MAD VLAN.
	• If no intermediate device is used, connect each IRF member device to all other member devices.
	• As a best practice, do not use the ND MAD VLAN for any other purposes.

ND MAD and feature configuration	If an intermediate device is used, make sure the following requirements are met: • Run the spanning tree feature between the IRF fabric and the intermediate device to ensure that there is only one ND MAD link in forwarding state. For more information about the spanning tree feature and its configuration, see *Layer 2—LAN Switching Configuration Guide*. • Enable the IRF fabric to change its bridge MAC address as soon as the address owner leaves. • If the intermediate device is also an IRF fabric, assign the two IRF fabrics different domain IDs for correct split detection.

When you configure ND MAD on a management Ethernet port, follow these restrictions and guidelines:

Category	Restrictions and guidelines
Management Ethernet ports for ND MAD	Connect a management Ethernet port on each member device to the common Ethernet ports on the intermediate device.
ND MAD VLAN	On the intermediate device, create a VLAN for ND MAD, and assign the ports used for ND MAD to the VLAN. On the IRF fabric, you do not need to assign the management Ethernet ports to the VLAN.
ND MAD and feature configuration	• Enable the IRF fabric to change its bridge MAC address as soon as the address owner leaves. • If the intermediate device is also an IRF fabric, assign the two IRF fabrics different domain IDs for correct split detection.

When you use the **mad nd enable** command, the system prompts you to enter a domain ID. If you do not want to change the current domain ID, press **enter** at the prompt.

An IRF fabric has only one IRF domain ID. You can change the IRF domain ID by using the following commands: **irf domain**, **mad enable**, **mad arp enable**, or **mad nd enable**. The IRF domain IDs configured by using these commands overwrite each other.

Examples

Enable ND MAD on VLAN-interface 3.

```
<Sysname> system-view
[Sysname] interface vlan-interface 3
[Sysname-Vlan-interface3] mad nd enable
You need to assign a domain ID (range: 0-4294967295)
[Current domain is: 0]: 1
The assigned domain ID is: 1
```

Related commands

irf domain

mad restore

Use **mad restore** to restore the normal MAD state of the IRF fabric in Recovery state.

Syntax

mad restore

Views

System view

Predefined user roles

network-admin

Usage guidelines

If the active IRF fabric has failed to work before the IRF split problem is fixed, use this command to restore an IRF fabric in Recovery state. The recovered IRF fabric will take over the active IRF fabric role.

Examples

Restore the normal MAD state of the IRF fabric in Recovery state.

```
<Sysname> system-view
[Sysname] mad restore
This command will restore the device from multi-active conflict state. Continue? [Y/N]:Y
Restoring from multi-active conflict state, please wait...
```

port group interface

Use **port group interface** to bind a physical interface to an IRF port.

Use **undo port group interface** to remove the binding of a physical interface to an IRF port.

Syntax

port group interface *interface-type interface-number*

undo port group interface *interface-name*

Default

No physical interfaces are bound to an IRF port.

Views

IRF port view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies a physical interface by its type and number.

interface-name: Specifies a physical interface in the *interface-typeinterface-number* format. No space is allowed between the *interface-type* and *interface-number* arguments.

Usage guidelines

CAUTION:

Use the **undo port group interface** command with caution. If the physical interface is the only up member interface of the IRF port, the IRF fabric will split after you remove the binding.

Execute this command multiple times to bind multiple physical interfaces to an IRF port. You can bind a maximum of eight physical interfaces to an IRF port. However, you might be unable to bind as many as eight physical interfaces to an IRF port due to hardware restrictions. For more information about IRF physical port restrictions, see the installation guide for the device.

Use the **shutdown** command to shut down a physical interface before you bind it to or remove it from an IRF port. To bring up the physical interface after a binding or binding removal operation, use the **undo shutdown** command.

For more information about IRF port binding requirements, see *Virtual Technologies Configuration Guide*.

Examples

Bind Ten-GigabitEthernet 1/0/51 to IRF-port 1/1 on IRF member 1.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/51
[Sysname-Ten-GigabitEthernet1/0/51] shutdown
[Sysname-Ten-GigabitEthernet1/0/51] quit
[Sysname] irf-port 1/1
[Sysname-irf-port1/1] port group interface ten-gigabitethernet 1/0/51
[Sysname-irf-port1/1] quit
[Sysname] interface ten-gigabitethernet 1/0/51
[Sysname-Ten-GigabitEthernet1/0/51] undo shutdown
```

Related commands

irf-port

Layer 2—LAN Switching Command Reference

This command reference is applicable to the following switches and software versions:

H3C S5120V2-LI switch series (Release 6308P01 and later)
H3C S3100V3-SI switch series (Release 6309P01 and later)
H3C S5110V2 switch series (Release 6310 and later)
H3C S5110V2-SI switch series (Release 6310 and later)
H3C S5000V3-EI switch series (Release 6310 and later)
H3C S5000V5-EI switch series (Release 6319P01 and later)
H3C S5000E-X switch series (Release 6310 and later)
H3C S5130S-LI switch series (Release 6310 and later)
H3C MS4320V2 switch series (Release 6308P01 and later)
H3C MS4320 switch series (Release 6308P01 and later)
H3C MS4300V2 switch series (Release 6308P01 and later)
H3C MS4200 switch series (Release 6310 and later)
H3C WS5810-WiNet switch series (Release 6308P01 and later)
H3C WS5820-WiNet switch series (Release 6308P01 and later)
H3C WAS6000 switch series (Release 6308P01 and later)
H3C S5000X-EI switch series (Release 6329 and later)
H3C MS4320V3 switch series (Release 6329 and later)
H3C S5120V3-SI switch series (Release 6329 and later)
H3C S5120V3-LI switch series (Release 6329 and later)

New H3C Technologies Co., Ltd.
http://www.h3c.com

Software version: Release 63xx
Document version: 6W105-20230524

Preface

This command reference describes Layer 2—LAN switching configuration commands.

This preface includes the following topics about the documentation:

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Documentation feedback

You can e-mail your comments about product documentation to info@h3c.com.

We appreciate your comments.

Contents

Ethernet interface commands

Common Ethernet interface commands

bandwidth

Use **bandwidth** to set the expected bandwidth of an interface.

Use **undo bandwidth** to restore the default.

Syntax

bandwidth *bandwidth-value*

undo bandwidth

Default

The expected bandwidth (in kbps) is the interface baud rate divided by 1000.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

bandwidth-value: Specifies the expected bandwidth in the range of 1 to 400000000 kbps.

Usage guidelines

The expected bandwidth is an informational parameter used only by higher-layer protocols for calculation. You cannot adjust the actual bandwidth of an interface by using this command.

Examples

Set the expected bandwidth of GigabitEthernet 1/0/1 to 1000 kbps.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] bandwidth 1000
```

Related commands

speed

broadcast-suppression

Use **broadcast-suppression** to enable broadcast suppression and set the broadcast suppression threshold.

Use **undo broadcast-suppression** to disable broadcast suppression.

Syntax

broadcast-suppression { *ratio* | **pps** *max-pps* | **kbps** *max-kbps* }

undo broadcast-suppression

Default

Ethernet interfaces do not suppress broadcast traffic.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

ratio: Sets the broadcast suppression threshold as a percentage of the interface bandwidth. The value range for this argument is 0 to 100. A smaller value means that less broadcast traffic is allowed to pass through.

pps *max-pps*: Specifies the maximum number of broadcast packets that the interface can forward per second. The value range for the *max-pps* argument (in pps) is 0 to 1.4881 × the interface bandwidth.

kbps *max-kbps*: Specifies the maximum number of kilobits of broadcast traffic that the Ethernet interface can forward per second. The value range for this argument (in kbps) is 0 to the interface bandwidth.

Usage guidelines

The broadcast storm suppression features limits the size of broadcast traffic to a threshold on an interface. When the broadcast traffic on the interface exceeds this threshold, the system drops packets until the traffic drops below this threshold.

Both the **storm-constrain** command and the **broadcast-suppression** command can suppress broadcast storms on a port. The **broadcast-suppression** command uses the chip to physically suppress broadcast traffic. It has less influence on the device performance than the **storm-constrain** command, which uses software to suppress broadcast traffic.

For the traffic suppression result to be determined, do not configure both the **storm-constrain broadcast** command and the **broadcast-suppression** command on an interface.

When you configure the suppression threshold in kbps, the actual suppression threshold might be different from the configured one as follows:

- If the configured value is smaller than 64, the value of 64 takes effect.
- If the configured value is greater than 64 but not an integer multiple of 64, the integer multiple of 64 that is greater than and closest to the configured value takes effect.

For the suppression threshold that takes effect, see the prompt on the device.

Examples

Set the broadcast suppression threshold to 10000 kbps on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] broadcast-suppression kbps 10000
The actual value is 10048 on port GigabitEthernet1/0/1 currently.
```

The output shows that the value that takes effect is 10048 kbps (157 times of 64), because the chip only supports step 64.

Related commands

multicast-suppression

unicast-suppression

combo enable

Use **combo enable** to activate the copper or fiber combo port of a combo interface.

Syntax

combo enable { **auto** | **copper** | **fiber** }

Default

The copper or fiber combo port is automatically activated depending on the medium inserted in the combo interface.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

auto: Automatically identifies the media inserted and activates the corresponding combo port.

copper: Activates the copper combo port. In this case, use twisted pairs to connect the port.

fiber: Activates the fiber combo port. In this case, use optical fibers to connect the port.

Usage guidelines

A combo interface is a logical interface that physically contains one fiber combo port and one copper combo port on the device panel. The two ports share one forwarding interface. As a result, they cannot work simultaneously. When you activate either port, the other port is automatically disabled. You can select to activate the copper combo port or fiber combo port.

This command is available only on devices that support combo interfaces.

If you execute the **combo enable auto** command on a combo interface and the combo interface is connected to cables or optical fibers, you can use the **display interface** command to display the interface information.

- If the **display interface** command output contains "Media type is twisted pair," the copper combo port is activated.
- Otherwise, the fiber combo port is activated.

Before using this command, perform the following tasks according to the marks on the device panel:

- Determine the combo interfaces on your device.
- Identify the two physical interfaces that belong to each combo interface.

Examples

Activate the copper combo port of combo interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] combo enable copper
```

Activate the fiber combo port of combo interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] combo enable fiber
```

dampening

Use **dampening** to enable the device to dampen an interface when the interface is flapping.

Use **undo dampening** to restore the default.

Syntax

dampening [*half-life reuse suppress max-suppress-time*]

undo dampening

Default

Interface dampening is disabled on Ethernet interfaces.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

half-life: Specifies the amount of time after which a penalty is decreased, in the range of 1 to 120 seconds. The default value is 54 seconds.

reuse: Specifies the reuse threshold in the range of 200 to 20000. The default value is 750. The reuse threshold must be less than the suppression threshold.

suppress: Specifies the suppression threshold in the range of 200 to 20000. The default value is 2000.

max-suppress-time: Specifies the maximum amount of time the interface can be dampened, in the range of 1 to 255 seconds. The default value is 162 seconds (three times the half-life timer).

Usage guidelines

When configuring the **dampening** command, follow these rules to set the values mentioned above:

- The ceiling is equal to 2 (Max-suppress-time/Decay) × reuse-limits. It is not user configurable.
- The configured suppress limit is lower than or equal to the ceiling.
- The ceiling is lower than or equal to the maximum suppress limit supported.

This command, the **link-delay** command, and the **port link-flap protect enable** command are mutually exclusive on an interface.

This command does not take effect on the administratively down events. When you execute the **shutdown** command, the penalty restores to 0, and the interface reports the down event to the higher layer protocols.

Do not enable the dampening function on an interface with RRPP, MSTP, or Smart Link enabled. The S5000E-X, S5000X-EI, S5110V2-SI, S5000V3-EI, S5000V5-EI, and WAS6000 switches do not support RRPP or Smart Link.

After an interface in down state is dampened, the interface state displayed through the **display interface** command is always down.

Examples

Enable interface dampening on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dampening
```

Enable interface dampening on GigabitEthernet 1/0/1, and set the following parameters:

- Half life time to 2 seconds.
- Reuse value to 800.
- Suppression threshold to 3000.
- Maximum suppression interval to 5 seconds.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dampening 2 800 3000 5
```

Related commands

display interface

link-delay

port link-flap protect enable

default

Use **default** to restore the default settings for an interface.

Syntax

default

Views

Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

CAUTION:

The **default** command might interrupt ongoing network services. Make sure you are fully aware of the impacts of this command when you use it in a live network.

This command might fail to restore the default settings for some commands because of command dependencies or system restrictions. You can use the **display this** command in interface view to identify these commands, and use their **undo** forms or follow the command reference to restore their default settings. If your restoration attempt still fails, follow the error message instructions to solve the problem.

Examples

Restore the default settings for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] default
```

description

Use **description** to configure the description of an interface.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

The description of an interface is the interface name plus **Interface** (for example, **GigabitEthernet1/0/1 Interface**).

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

text: Specifies the interface description, a case-sensitive string of 1 to 255 characters.

Examples

Set the description of GigabitEthernet 1/0/1 to **lan-interface**.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] description lan-interface
```

display counters

Use **display counters** to display interface traffic statistics.

Syntax

display counters { **inbound** | **outbound** } **interface** [*interface-type* [*interface-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

inbound: Displays inbound traffic statistics.

outbound: Displays outbound traffic statistics.

interface-type: Specifies an interface type.

interface-number: Specifies an interface number.

Usage guidelines

To clear the Ethernet interface traffic statistics, use the **reset counters interface** command.

If you do not specify an interface type, this command displays traffic statistics for all interfaces that have traffic counters.

If you specify an interface type but do not specify an interface number, this command displays traffic statistics for all interfaces of the specified type.

If you specify an interface type and number, this command displays traffic statistics for the specified interface.

Examples

Display inbound traffic statistics for all interfaces.

```
<Sysname> display counters inbound interface
Interface            Total (pkts)    Broadcast (pkts)    Multicast (pkts)  Err (pkts)
GE1/0/1                       100                 100                   0           0
GE1/0/2                  Overflow            Overflow            Overflow    Overflow

 Overflow: More than 14 digits (7 digits for column "Err").
       --: Not supported.
```

Table 1 Command output

Field	Description
Interface	Abbreviated interface name.
Total (pkts)	Total number of packets received or sent through the interface.
Broadcast (pkts)	Total number of broadcast packets received or sent through the interface.
Multicast (pkts)	Total number of multicast packets received or sent through the interface.
Err (pkts)	Total number of error packets received or sent through the interface.
Overflow: More than 14 digits (7 digits for column "Err")	The command displays **Overflow** when any of the following conditions exist: • The data length of an **Err** field value is greater than 7 decimal digits. • The data length of a non-Err field value is greater than 14 decimal digits.
--: Not supported	The statistical item is not supported.

Related commands

`reset counters interface`

display counters rate

Use **`display counters rate`** to display traffic rate statistics for interfaces in up state for the most recent statistics polling interval.

Syntax

`display counters rate` { **`inbound`** | **`outbound`** } **`interface`** [*`interface-type`* [*`interface-number`*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

`inbound`: Displays inbound traffic rate statistics.

`outbound`: Displays outbound traffic rate statistics.

`interface-type`: Specifies an interface type.

interface-number: Specifies an interface number.

Usage guidelines

If you do not specify an interface type, this command displays traffic rate statistics for all up interfaces that have traffic counters.

If you specify an interface type but do not specify an interface number, this command displays traffic rate statistics for all up interfaces of the specified type.

If you specify an interface type and an interface, this command displays traffic rate statistics for the specified interface.

If an interface that you specify is always down for the most recent statistics polling interval, the system prompts that the interface does not support the command.

To set the statistics polling interval, use the **flow-interval** command.

Examples

Display the inbound traffic rate statistics for all interfaces.

```
<Sysname> display counters rate inbound interface
Usage: Bandwidth utilization in percentage
Interface            Usage (%)   Total (pps)   Broadcast (pps)   Multicast (pps)
GE1/0/1                      0             0                --                --

 Overflow: More than 14 digits.
       --: Not supported.
```

Table 2 Command output

Field	Description
Interface	Abbreviated interface name.
Usage (%)	Bandwidth usage (in percentage) of the interface for the last statistics polling interval.
Total (pps)	Average receiving or sending rate (in pps) for unicast packets for the last statistics polling interval.
Broadcast (pps)	Average receiving or sending rate (in pps) for broadcast packets for the last statistics polling interval.
Multicast (pps)	Average receiving or sending rate (in pps) for multicast packets for the last statistics polling interval. .
Overflow: more than 14 decimal digits	The command displays **Overflow** if the data length of a statistical item is greater than 14 decimal digits.
--: not supported	The statistical item is not supported.

Related commands

flow-interval

reset counters interface

display ethernet statistics

Use **display ethernet statistics** to display the Ethernet module statistics.

Syntax

display ethernet statistics slot *slot-number*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number:* Specifies an IRF member device by its member ID.

Examples

Display the Ethernet module statistics for the specified slot.

```
<Sysname> display ethernet statistics slot 1
ETH receive packet statistics:
    Totalnum        : 10447          ETHIINum     : 4459
    SNAPNum         : 0              RAWNum       : 0
    LLCNum          : 0              UnknownNum   : 0
    ForwardNum      : 4459           ARP          : 0
    MPLS            : 0              ISIS         : 0
    ISIS2           : 0              IP           : 0
    IPV6            : 0
ETH receive error statistics:
    NullPoint       : 0              ErrIfindex   : 0
    ErrIfcb         : 0              IfShut       : 0
    ErrAnalyse      : 5988           ErrSrcMAC    : 5988
    ErrHdrLen       : 0

ETH send packet statistics:
    L3OutNum        : 211            VLANOutNum   : 0
    FastOutNum      : 155            L2OutNum     : 0
ETH send error statistics:
    MbufRelayNum    : 0              NullMbuf     : 0
    ErrAdjFwd       : 0              ErrPrepend   : 0
    ErrHdrLen       : 0              ErrPad       : 0
    ErrQoSTrs       : 0              ErrVLANTrs   : 0
    ErrEncap        : 0              ErrTagVLAN   : 0
    IfShut          : 0              IfErr        : 0
```

Table 3 Output description

Field	Description
ETH receive packet statistics	Statistics about the Ethernet packets received by the Ethernet module: • **Totalnum**—Total number of received packets. • **ETHIINum**—Number of packets encapsulated by using Ethernet II. • **SNAPNum**—Number of packets encapsulated by using SNAP. • **RAWNum**—Number of packets encapsulated by using RAW. • **ISISNum**—Number of packets encapsulated by using ISIS. This field is not supported in the current software version. • **LLCNum**—Number of packets encapsulated by using LLC. • **UnknownNum**—Number of packets encapsulated by using unknown methods.

Field	Description
	• **ForwardNum**—Number of packets forwarded at Layer 2 or sent to the CPU. • **ARP**—Number of ARP packets. • **MPLS**—Number of MPLS packets. This field is not supported in the current software version. • **ISIS**—Number of IS-IS packets. This field is not supported in the current software version. • **ISIS2**—Number of large 802.3/802.2 frames encapsulated by using IS-IS. This field is not supported in the current software version. • **IP**—Number of IP packets. • **IPv6**—Number of IPv6 packets.
ETH receive error statistics	Statistics about the error Ethernet packets in the inbound direction on the Ethernet module. Errors might be included in packets or occur during the receiving process. The items include: • **NullPoint**—Number of packets that include null pointers. • **ErrIfindex**—Number of packets that include incorrect interface indexes. • **ErrIfcb**—Number of packets that include incorrect interface control blocks. • **IfShut**—Number of packets that are being received when the interface is shut down. • **ErrAnalyse**—Number of packets that include packet parsing errors. • **ErrSrcMAC**—Number of packets that include incorrect source MAC addresses. • **ErrHdrLen**—Number of packets that include header length errors.
ETH send packet statistics	Statistics about the Ethernet packets sent by the Ethernet module: • **L3OutNum**—Number of packets sent out of Layer 3 Ethernet interfaces. This field is not supported in the current software version. • **VLANOutNum**—Number of packets sent out of VLAN interfaces. • **FastOutNum**—Number of packets fast forwarded. • **L2OutNum**—Number of packets sent out of Layer 2 Ethernet interfaces. • **MbufRelayNum**—Number of packets transparently sent.
ETH send error statistics	Statistics about the error Ethernet packets in the outbound direction on the Ethernet module: • **NullMbuf**—Number of packets with null pointers. • **ErrAdjFwd**—Number of packets with adjacency table errors. • **ErrPrepend**—Number of packets with extension errors. • **ErrHdrLen**—Number of packets with header length errors. • **ErrPad**—Number of packets with padding errors. • **ErrQoSTrs**—Number of packets that failed to be sent by QoS. • **ErrVLANTrs**—Number of packets that failed to be sent in VLANs. • **ErrEncap**—Number of packets that failed to be sent due to link header encapsulation failures. • **ErrTagVLAN**—Number of packets that failed to be sent due to VLAN tag encapsulation failures. • **IfShut**—Number of packets that are being sent when the interface is shut down. • **IfErr**—Number of packets with incorrect outgoing interfaces.

Related commands

`reset ethernet statistics`

display interface

Use **display interface** to display interface information.

Syntax

display interface [*interface-type* [*interface-number*]] [**brief** [**description** | **down**]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type: Specifies an interface type.

interface-number: Specifies an interface number.

brief: Displays brief interface information. If you do not specify this keyword, the command displays detailed interface information.

description: Displays complete interface descriptions. If you do not specify this keyword, the command displays only the first 27 characters of each interface description.

down: Displays information about interfaces in down state and the causes. If you do not specify this keyword, the command displays information about interfaces in all states.

Usage guidelines

If you do not specify an interface type, this command displays information about all interfaces.

If you specify an interface type but do not specify an interface number, this command displays information about all interfaces of the specified type.

Examples

Display detailed information about Layer 2 interface GigabitEthernet 1/0/1.

```
<Sysname> display interface gigabitethernet 1/0/1
GigabitEthernet1/0/1
Current state: DOWN
Line protocol state: DOWN
IP packet frame type: Ethernet II, hardware address: 000c-2963-b767
Description: GigabitEthernet1/0/1 Interface
Bandwidth: 100000 kbps
Loopback is not set
Media type is twisted pair, port hardware type is 1000_BASE_T_AN_SFP
Unknown-speed mode, unknown-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
Flow-control is not enabled
Maximum frame length: 9216
Allow jumbo frame to pass
Broadcast max-ratio: 100%
Multicast max-ratio: 100%
Unicast max-ratio: 100%
PVID: 1
```

```
MDI type: Automdix
Port link-type: Access
 Tagged VLANs:   None
 UnTagged VLANs: 1
Port priority: 2
Last link flapping: 6 hours 39 minutes 25 seconds
Last clearing of counters:  14:34:09 Tue 11/01/2011
Current system time:2018-08-10 14:58:27
Last time when physical state changed to up:-
Last time when physical state changed to down:2018-08-10 14:57:58
 Peak input rate: 0 bytes/sec, at 2013-07-17 22:06:19
 Peak output rate: 0 bytes/sec, at 2013-07-17 22:06:19
 Last 300 seconds input:  0 packets/sec 0 bytes/sec -%
 Last 300 seconds output:  0 packets/sec 0 bytes/sec -%
 Input (total):  0 packets, 0 bytes
          0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Input (normal):  0 packets, 0 bytes
          0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Input:  0 input errors, 0 runts, 0 giants, 0 throttles
          0 CRC, 0 frame, 0 overruns, 0 aborts
          0 ignored, 0 parity errors
 Output (total): 0 packets, 0 bytes
          0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Output (normal): 0 packets, 0 bytes
          0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Output: 0 output errors, 0 underruns, 0 buffer failures
          0 aborts, 0 deferred, 0 collisions, 0 late collisions
          0 lost carrier, 0 no carrier
```

Table 4 Command output

Field	Description
Current state	Physical link state of the interface: • **Administratively DOWN**—The interface has been shut down by using the **shutdown** command. • **DOWN**—The interface is administratively up, but its physical state is down (possibly because no physical link exists or the link has failed). • **DOWN (Link-Aggregation interface down)**—The aggregate interface to which the interface belongs has been shut down by using the **shutdown** command. • **DOWN (Monitor-Link uplink down)**—The interface has been shut down by Monitor Link. • **mac-address moving down**—The interface has been shut down by the MAC address move suppression feature. • **MAD ShutDown**—The interface has been shut down by IRF MAD. This state occurs if the interface is on an IRF fabric placed in Recovery state after an IRF split. • **OFP DOWN**—The interface has been shut down by OpenFlow. • **Storm-Constrain**—The interface has been shut down because the storm control feature detected that unknown

Field	Description
	unicast traffic, multicast traffic, or broadcast traffic exceeded the upper threshold. • **STP DOWN**—The interface has been shut down by the BPDU guard feature. • **UP**—The interface is both administratively and physically up.

Line protocol state	Data link layer state of the interface. The state is determined through automatic parameter negotiation at the data link layer.
	• **UP**—The data link layer protocol is up.
	• **UP (spoofing)**—The data link layer protocol is up, but the link is an on-demand link or does not exist. This attribute is typical of null interfaces and loopback interfaces.
	• **DOWN**—The data link layer protocol is down.
	• **DOWN (***protocols***)**—The data link layer has been shut down by protocols included in the parentheses. Available protocols include:
	  ○ **DLDP**—Shuts down the data link layer when it detects that the link is unidirectional.
	  ○ **OAM**—Shuts down the data link layer when it detects a remote link failure.
	  ○ **LAGG**—Shuts down the data link layer when it detects that the aggregate interface does not have Selected ports.
	  ○ **BFD**—Shuts down the data link layer when it detects a link failure.

Bandwidth	Expected bandwidth of the interface.
Maximum transmission unit	MTU of the interface.
IP packet frame type	IPv4 packet framing format.
hardware address	MAC address of the interface.
Port priority	Port priority of the interface.
Loopback is set internal	An internal loopback test is running on the interface. This field depends on your configuration.
Loopback is set external	An external loopback test is running on the interface. This field depends on your configuration.
Loopback is not set	No loopback test is running on the interface. This field depends on your configuration.
10Mbps-speed mode	The interface is operating at 10 Mbps. This field depends on your configuration and the link parameter negotiation result.
100Mbps-speed mode	The interface is operating at 100 Mbps. This field depends on your configuration and the link parameter negotiation result.
1000Mbps-speed mode	The interface is operating at 1000 Mbps. This field depends on your configuration and the link parameter negotiation result.
10Gbps-speed mode	The interface is operating at 10 Gbps. This field depends on your configuration and the link parameter negotiation result.
Unknown-speed mode	The speed of the interface is unknown because the speed negotiation fails or the interface is physically disconnected.
half-duplex mode	The interface is operating in half duplex mode. This field depends on your configuration and the link parameter negotiation result.
full-duplex mode	The interface is operating in full duplex mode. This field depends

Field	Description
	on your configuration and the link parameter negotiation result.
unknown-duplex mode	The duplex mode of the interface is unknown because the duplex mode negotiation fails or the interface is physically disconnected.
Link speed type is autonegotiation	The interface is configured with the **speed auto** command.
Link speed type is force link	The interface is manually configured with a speed (for example, 1000 Mbps) by using the **speed** command.
link duplex type is autonegotiation	The interface is configured with the **duplex auto** command.
link duplex type is force link	The interface is manually configured with a duplex mode (for example, half or full) by using the **duplex** command.
Flow-control is not enabled	Generic flow control is disabled on the interface. This field depends on your configuration and the link parameter negotiation result.
Maximum frame length	Maximum length of Ethernet frames allowed to pass through the interface.
Allow jumbo frame to pass	The interface allows jumbo frames to pass through.
Broadcast max-	Broadcast storm suppression threshold in ratio, pps, or kbps. The unit of the threshold depends on your configuration.
Multicast max-	Multicast storm suppression threshold in ratio, pps, or kbps. The unit of the threshold depends on your configuration.
Unicast max-	Unknown unicast storm suppression threshold in ratio, pps, or kbps. The unit of the threshold depends on your configuration.
PVID	Port VLAN ID (PVID) of the interface.
MDI type	MDIX mode of the interface: • automdix. • mdi. • mdix.
Port link-type	Link type of the interface: • access. • trunk. • hybrid.
Tagged VLANs	VLANs for which the interface sends packets without removing VLAN tags.
Untagged VLANs	VLANs for which the interface sends packets after removing VLAN tags.
VLAN Passing	VLANs whose packets can be forwarded by the port. The VLANs must have been created.
VLAN permitted	VLANs whose packets are permitted by the port.
Trunk port encapsulation	Encapsulation protocol type for the trunk port.
Last link flapping	The amount of time that has elapsed since the most recent physical state change of the interface. This field displays **Never** if the interface has been physically down since device startup.
Last clearing of counters	Time when the **reset counters interface** command was last used to clear the interface statistics. This field displays **Never** if the **reset counters interface** command has never been used on the interface since device startup.

Field	Description
Current system time	Current system time in the YYYY/MM/DD HH:MM:SS format. If the time zone is configured, this field is in the YYYY/MM/DD HH:MM:SS *zone-name*±HH:MM:SS format, where the *zone-name* argument is the local time zone.
Last time when physical state changed to up	Last time when the physical state of the interface changed to up. If the time zone is configured, this field is in the YYYY/MM/DD HH:MM:SS *zone-name*±HH:MM:SS format, where the *zone-name* argument is the local time zone. A hyphen (-) indicates that the physical state of the interface has never changed.
Last time when physical state changed to down	Last time when the physical state of the interface changed to down. If the time zone is configured, this field is in the YYYY/MM/DD HH:MM:SS *zone-name*±HH:MM:SS format, where the *zone-name* argument is the local time zone. A hyphen (-) indicates that the physical state of the interface has never changed.
Last 300 seconds input: 0 packets/sec 0 bytes/sec 0% Last 300 seconds output: 0 packets/sec 0 bytes/sec 0%	Average inbound or outbound traffic rate (in pps and Bps) in the last 300 seconds, and the ratio of the actual rate to the interface bandwidth. A hyphen (-) indicates that the statistical item is not supported.
Input(total): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	The two fields on the first line represent the inbound traffic statistics (in packets and bytes) for the interface. All inbound normal packets, abnormal packets, and normal pause frames were counted. The four fields on the second line represent: • Number of inbound unicast packets. • Number of inbound broadcasts. • Number of inbound multicasts. • Number of inbound pause frames. A hyphen (-) indicates that the statistical item is not supported.
Input(normal): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	The two fields on the first line represent the inbound normal traffic and pause frame statistics (in packets and bytes) for the interface. The four fields on the second line represent: • Number of inbound normal unicast packets. • Number of inbound normal broadcasts. • Number of inbound normal multicasts. • Number of inbound normal pause frames. A hyphen (-) indicates that the statistical item is not supported.
input errors	Statistics of incoming error packets.
runts	Number of inbound frames meeting the following conditions: • Shorter than 64 bytes. • In correct format. • Containing valid CRCs.
giants	Number of inbound giants. Giants refer to frames larger than the maximum frame length supported on the interface. For an Ethernet interface that does not permit jumbo frames, the maximum frame length is as follows: • 1518 bytes (without VLAN tags). • 1522 bytes (with VLAN tags).

Field	Description
	For an Ethernet interface that permits jumbo frames, the maximum Ethernet frame length is set when you configure jumbo frame support on the interface.
throttles	Number of inbound frames that had a non-integer number of bytes.
CRC	Total number of inbound frames that had a normal length, but contained CRC errors.
frame	Total number of inbound frames that contained CRC errors and a non-integer number of bytes.
overruns	Number of packets dropped because the input rate of the port exceeded the queuing capability.

aborts	Total number of illegal inbound packets:
	• **Fragment frames**—CRC error frames shorter than 64 bytes. The length (in bytes) can be an integral or non-integral value.
	• **Jabber frames**—CRC error frames greater than the maximum frame length supported on the Ethernet interface (with an integral or non-integral length).
	  ○ For an Ethernet interface that does not permit jumbo frames, the maximum frame length is 1518 bytes (without VLAN tags) or 1522 bytes (with VLAN tags).
	  ○ For an Ethernet interface that permits jumbo frames, the maximum Ethernet frame length is set when you configure jumbo frame support on the interface.
	• **Symbol error frames**—Frames that contained a minimum of one undefined symbol.
	• **Unknown operation code frames**—Non-pause MAC control frames.
	• **Length error frames**—Frames whose 802.3 length fields did not match the actual frame length (46 to 1500 bytes).

ignored	Number of inbound frames dropped because the receiving buffer of the port ran low.
parity errors	Total number of frames with parity errors.
Output(total): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	The two fields on the first line represent the outbound traffic statistics (in packets and bytes) for the interface. All outbound normal packets, abnormal packets, and normal pause frames were counted. The four fields on the second line represent: • Number of outbound unicast packets. • Number of outbound broadcasts. • Number of outbound multicasts. • Number of outbound pause frames. A hyphen (-) indicates that the statistical item is not supported.
Output(normal): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	The two fields on the first line represent the outbound normal traffic and pause frame statistics (in packets and bytes) for the interface. The four fields on the second line represent: • Number of outbound normal unicast packets. • Number of outbound normal broadcasts. • Number of outbound normal multicasts. • Number of outbound normal pause frames.

Field	Description
	A hyphen (-) indicates that the statistical item is not supported.
output errors	Number of outbound packets with errors.
underruns	Number of packets dropped because the output rate of the interface exceeded the output queuing capability. This is a low-probability hardware anomaly.
buffer failures	Number of packets dropped because the transmitting buffer of the interface ran low.
aborts	Number of packets that failed to be transmitted, for example, because of Ethernet collisions.
deferred	Number of frames that the interface deferred to transmit because of detected collisions.
collisions	Number of frames that the interface stopped transmitting because Ethernet collisions were detected during transmission.
late collisions	Number of frames that the interface deferred to transmit after transmitting their first 512 bits because of detected collisions.
lost carrier	Number of carrier losses during transmission. This counter increases by one when a carrier is lost, and applies to serial WAN interfaces.
no carrier	Number of times that the port failed to detect the carrier when attempting to send frames. This counter increases by one when a port failed to detect the carrier, and applies to serial WAN interfaces.
Peak input rate	Peak rate of inbound traffic in Bps, and the time when the peak inbound traffic rate occurred.
Peak output rate	Peak rate of outbound traffic in Bps, and the time when the peak outbound traffic rate occurred.

Display brief information about all interfaces.

```
<Sysname> display interface brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) – spoofing

Interface            Link Protocol Primary IP      Description
Loop0                UP   UP(s)    2.2.2.9
NULL0                UP   UP(s)    --
Vlan1                UP   DOWN     --
Vlan999              UP   UP       192.168.1.42

Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) - auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface            Link Speed   Duplex Type PVID Description
GE1/0/2              DOWN auto    A      A    1
GE1/0/3              UP   auto    F(a)   A    1    aaaaaaaaaaaaaaaaaaaaaaaaaa
```

Display brief information about GigabitEthernet 1/0/3, including the complete description of the interface.

```
<Sysname> display interface gigabitethernet 1/0/3 brief description
Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) - auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface            Link Speed   Duplex Type PVID Description
GE1/0/3              UP   auto    F(a)   A    1    aaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Display information about interfaces in DOWN state and the causes.

```
<Sysname> display interface brief down
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Interface            Link Cause
Vlan2                DOWN Not connected

Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Interface            Link Cause
GE1/0/2              DOWN Not connected
```

Table 5 Command output

Field	Description
Interface	Interface name.
Link	Physical link state of the interface: • **UP**—The interface is physically up. • **DOWN**—The interface is physically down. • **ADM**—The interface has been shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **Stby**—The interface is a backup interface in standby state.
Protocol	Data link layer protocol state of the interface: • **UP**—The data link layer protocol of the interface is up. • **DOWN**—The data link layer protocol of the interface is down. • **UP(s)**—The data link layer protocol of the interface is up, but the link is an on-demand link or does not exist. The **(s)** attribute represents the spoofing flag. This value is typical of null interfaces and loopback interfaces.
Primary IP	Primary IP address of the interface. This field displays two hyphens (**--**) if the interface does not have an IP address.
Description	Description of the interface.
Brief information of interfaces in bridge mode:	Brief information about Layer 2 interfaces.
Type: A - access; T - trunk; H – hybrid	Link type options for interfaces.
Speed	Speed of the interface, in bps.

Field	Description
	This field displays the **(a)** flag next to the speed if the speed is automatically negotiated. This field displays **auto** if the interface is configured to autonegotiate its speed but the autonegotiation has not started.
Duplex	Duplex mode of the interface: • **A**—Autonegotiation. The interface is configured to autonegotiate its duplex mode but the autonegotiation has not started. • **F**—Full duplex. • **F(a)**—Autonegotiated full duplex. • **H**—Half duplex. • **H(a)**—Autonegotiated half duplex.
Type	Link type of the interface: • **A**—Access. • **H**—Hybrid. • **T**—Trunk.
PVID	Port VLAN ID.
Cause	Cause for the physical link state of an interface to be **DOWN**: • **Administratively**—The interface has been manually shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **DOWN (Link-Aggregation interface down)**—The interface is a member port of an aggregate interface, and the aggregate interface is down. • **DOWN (Loopback detection down)**—The loopback detection module has detected loops. • **DOWN (Monitor-Link uplink down)**—The monitor link module has detected that the uplink is down. • **MAD ShutDown**—The interface is on an IRF fabric placed by IRF MAD in Recovery state after an IRF split. • **Not connected**—No physical connection exists (possibly because the network cable is disconnected or faulty). • **Storm-Constrain**—The storm control feature has detected that unknown unicast traffic, multicast traffic, or broadcast traffic exceeded the upper threshold. • **STP DOWN**—The interface has been shut down by the BPDU guard feature. • **Port Security Disabled**—The interface has been shut down by the intrusion detection mechanism because the interface received illegal packets. • **OFP DOWN**—The interface has been shut down by OpenFlow.

Related commands

reset counters interface

display interface link-info

Use **display interface link-info** to display the status and packet statistics of interfaces.

Syntax

display interface link-info

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display status and statistics of all interfaces.

```
<Sysname> display interface link-info
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface        Link Protocol  InUsage OutUsage         InErrs        OutErrs
GE1/0/1          UP   UP            10%       0%              0              0
NULL0            UP   UP(s)          0%       0%              0              0

 Overflow: More than 7 digits.
       --: Not supported.
```

Table 6 Command output

Field	Description
Link: ADM - administratively down; Stby - standby	Physical link state of the interface: • **ADM**—The interface has been shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **Stby**—The interface is a backup interface in standby state. To see the primary interface, use the **display interface-backup state** command.
Protocol: (s) – spoofing	The data link layer protocol of the interface is up, but the link is an on-demand link or does not exist. The **(s)** attribute represents the spoofing flag. This value is typical of null interfaces, loopback interfaces, and InLoopback interfaces.
Interface	Abbreviated interface name.
Link	Physical link state of the interface: • **UP**—The interface is physically up. • **DOWN**—The interface is physically down. • **ADM**—The interface has been shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **Stby**—The interface is a backup interface in standby state.
Protocol	Data link layer protocol state of the interface: • **UP**—The data link layer protocol of the interface is up. • **DOWN**—The data link layer protocol of the interface is down. • **UP(s)**—The data link layer protocol of the interface is up, but the link is an on-demand link or does not exist. The **(s)** attribute represents the spoofing flag. This value is typical of null interfaces, loopback interfaces, and InLoopback interfaces.
InUsage	Inbound bandwidth usage within the most recent statistics polling interval. It is calculated by this formula: Average inbound speed of the interface within the most recent statistics polling interval/interface bandwidth. To set the statistics polling interval, use the **flow-interval** command.

Field	Description
OutUsage	Outbound bandwidth usage within the most recent statistics polling interval. It is calculated by this formula: Average outbound speed of the interface within the most recent statistics polling interval/interface bandwidth. To set the statistics polling interval, use the **flow-interval** command.
InErrs	Number of error packets received.
OutErrs	Number of error packets sent.
Overflow: More than 7 digits.	The data length of a statistical item value is greater than 7 decimal digits.
--: Not supported.	A hyphen (-) indicates that the corresponding statistical item is not supported.

Related commands

flow-interval

display link-flap protection

Use **display link-flap protection** to display information about link flapping protection on an interface.

Syntax

display link-flap protection [**interface** *interface-type* [*interface-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type: Specifies an interface type. If you do not specify an interface type, the command displays information about link flapping protection on all interfaces.

interface-number: Specifies an interface number. If you do not specify an interface number, the command displays information about link flapping protection on all interfaces of the specified type.

Examples

Display information about link flapping protection on all interfaces.

```
<Sysname> display link-flap protection
Link-flap protection: Enabled
Interface            Link-flap  Status  Interval  Threshold
GE1/0/1              Enabled    Down    10        5
GE1/0/2              Disabled   N/A     --        --
```

Table 7 Command output

Field	Description
Link-flap protection	Status of global link flapping protection: • **Enabled**—Link flapping protection is enabled globally.

Field	Description
	• **Disabled**—Link flapping protection is disabled globally.
Link-flap	Status of link flapping protection on an interface: • **Enabled**—Link flapping protection is enabled on an interface. • **Disabled**—Link flapping protection is disabled on an interface.
Status	Status of an interface: • **Down**—The interface has been shut down by the link flapping protection feature. • **N/A**—The interface status is not affected by the link flapping protection feature.
Interval	Link flapping detection interval for an interface.
Threshold	Link flapping detection threshold for an interface.

Related commands

link-flap protect enable

port link-flap protect enable

duplex

Use **duplex** to set the duplex mode for an Ethernet interface.

Use **undo duplex** to restore the default.

Syntax

duplex { **auto** | **full** | **half** }

undo duplex

Default

An Ethernet interface operates in autonegotiation mode.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

auto: Configures the interface to autonegotiate the duplex mode with the peer.

full: Configures the interface to operate in full duplex mode. In this mode, the interface can receive and transmit packets simultaneously.

half: Configures the interface to operate in half duplex mode. In this mode, the interface can only receive or transmit packets at a given time. Fiber ports, 1000-Mbps Ethernet interfaces, and 10000-Mbps Ethernet interfaces do not support this keyword.

Examples

Configure GigabitEthernet 1/0/1 to operate in full duplex mode.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] duplex full
```

eee enable

IMPORTANT:
Fiber ports do not support this command.

Use **eee enable** to enable Energy Efficient Ethernet (EEE) on an interface.

Use **undo eee enable** to disable EEE on an interface.

Syntax

eee enable

undo eee enable

Default

EEE is disabled.

Views

Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

With EEE enabled, a link-up interface enters low power state if it has not received any packet for a period of time. The time period depends on the chip specifications and is not configurable. When a packet arrives later, the interface restores to the normal state.

Examples

Enable EEE on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] eee enable
```

flow-control

Use **flow-control** to enable TxRx-mode generic flow control on an Ethernet interface.

Use **undo flow-control** to disable TxRx-mode generic flow control on the Ethernet interface.

Syntax

flow-control

undo flow-control

Default

TxRx-mode generic flow control is disabled on an Ethernet interface.

Views

Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

With TxRx-mode generic flow control configured, an interface can both send and receive flow control frames:

- When congested, the interface sends a flow control frame to its peer.
- Upon receiving a flow control frame from the peer, the interface suspends sending packets.

To implement flow control on a link, enable generic flow control at both ends of the link.

Examples

Enable TxRx-mode generic flow control on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] flow-control
```

flow-control receive enable

Use **flow-control receive enable** to enable Rx-mode generic flow control on an Ethernet port.

Use **undo flow-control** to disable Rx-mode generic flow control on an Ethernet port.

Syntax

flow-control receive enable

undo flow-control

Default

Rx-mode generic flow control is disabled on Ethernet interfaces.

Views

Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

With Rx-mode flow control enabled, an interface can receive but cannot send flow control frames.

- When the interface receives a flow control frame from its peer, it suspends sending packets to the peer.
- When traffic congestion occurs on the interface, it cannot send flow control frames to the peer.

To handle unidirectional traffic congestion on a link, configure the **flow-control receive enable** command at one end, and the **flow-control** command at the other. To enable both ends of the link to handle traffic congestion, configure the **flow-control** command at both ends.

Examples

Enable Rx-mode generic flow control on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-gigabitethernet 1/0/1] flow-control receive enable
```

Related commands

flow-control

flow-interval

Use **flow-interval** to set the statistics polling interval.

Use **undo flow-interval** to restore the default.

Syntax

flow-interval *interval*

undo flow-interval

Default

The statistics polling interval is 300 seconds.

Views

System view

Ethernet interface view

Predefined user roles

network-admin

Parameters

interval: Sets the statistics polling interval in seconds. The interval is in the range of 5 to 300 and must be a multiple of 5.

Usage guidelines

Configuring the statistics polling interval in system view is supported in only Release 6328 and later.

A device supports either the system view settings or the Ethernet interface view settings.

- The statistics polling interval configured in system view takes effect on all Ethernet interfaces.
- The statistics polling interval configured in Ethernet interface view takes effect only on the current interface.

For an Ethernet interface, the statistics polling interval configured in Ethernet interface view takes priority.

As a best practice, use the default setting when you set the statistics polling interval in system view. A short statistics polling interval might decrease the system performance and result in inaccurate statistics.

Examples

Set the statistics polling interval to 100 seconds on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] flow-interval 100
```

ifmonitor crc-error

Use **ifmonitor crc-error** to configure global CRC error packet alarm parameters.

Use **undo ifmonitor crc-error** to restore the default.

NOTE:

This command is supported only in Release 6340 and later.

Syntax

ifmonitor crc-error slot *slot-number* **high-threshold** *high-value* **low-threshold** *low-value* **interval** *interval* [**shutdown**]

undo ifmonitor crc-error slot *slot-number*

Default

The upper threshold is 1000, the lower threshold is 100, and the statistics collection and comparison interval is 10 seconds for CRC error packet alarms.

Views

System view

Predefined user roles

network-admin

Parameters

high-threshold *high-value*: Specifies the upper threshold for CRC error packet alarms, in the range of 1 to 4294967295 packets.

low-threshold *low-value*: Specifies the lower threshold for CRC error packet alarms, in the range of 1 to 4294967295 packets.

interval *interval*: Specifies the statistics collection and comparison interval for CRC error packets, in the range of 1 to 65535 seconds.

shutdown: Shuts down an interface when the number of incoming CRC error packets on the interface exceeds the upper threshold. Then, the interface stops forwarding all packets. To recover the interface, execute the **undo shutdown** command on the interface. If you do not specify this keyword, an upper threshold exceeding alarm is generated and the interface enters the alarm state when the number of incoming CRC error packets exceeds the upper threshold on the interface.

slot *slot-number*: Specifies an IRF member device by its member ID.

Usage guidelines

With the CRC error packet alarm function enabled, when the number of incoming CRC error packets on an interface in normal state within the specified interval exceeds the upper threshold, the interface generates an upper threshold exceeding alarm and enters the alarm state. When the number of incoming CRC error packets on an interface in the alarm state within the specified interval drops below the lower threshold, the interface generates a recovery alarm and restores to the normal state.

You can configure the CRC error packet alarm parameters in system view and interface view.

- The configuration in system view takes effect on all interfaces of the specified slot. The configuration in interface view takes effect only on the current interface.
- For an interface, the configuration in interface view takes priority, and the configuration in system view is used only when no configuration is made in interface view.

When you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the upper threshold to 5000, lower threshold to 400, and statistics collection and comparison interval to 6 seconds for CRC error packet alarms.

```
<Sysname> system-view
[Sysname] ifmonitor crc-error slot 1 high-threshold 5000 low-threshold 400 interval 6
```

Related commands

snmp-agent trap enable ifmonitor

ifmonitor input-error

Use **ifmonitor input-error** to configure global input error packet alarm parameters.

Use **undo ifmonitor input-error** to restore the default.

NOTE:
This command is supported only in Release 6340 and later.

Syntax

ifmonitor input-error slot *slot-number* **high-threshold** *high-value* **low-threshold** *low-value* **interval** *interval* [**shutdown**]

undo ifmonitor input-error slot *slot-number*

Default

The upper threshold is 1000, the lower threshold is 100, and the statistics collection and comparison interval is 10 seconds for input error packet alarms.

Views

System view

Predefined user roles

network-admin

Parameters

high-threshold *high-value*: Specifies the upper threshold for input error packet alarms, in the range of 1 to 4294967295 packets.

low-threshold *low-value*: Specifies the lower threshold for input error packet alarms, in the range of 1 to 4294967295 packets.

interval *interval*: Specifies the statistics collection and comparison interval for input error packets, in the range of 1 to 65535 seconds.

shutdown: Shuts down an interface when the number of input error packets on the interface exceeds the upper threshold. Then, the interface stops forwarding all packets. To recover the interface, execute the **undo shutdown** command on the interface. If you do not specify this keyword, an upper threshold exceeding alarm is generated and the interface enters the alarm state when the number of input error packets exceeds the upper threshold on the interface.

slot *slot-number*: Specifies an IRF member device by its member ID.

Usage guidelines

With the input error packet alarm function enabled, when the number of input error packets on an interface in normal state within the specified interval exceeds the upper threshold, the interface generates an upper threshold exceeding alarm and enters the alarm state. When the number of input error packets on an interface in the alarm state within the specified interval drops below the lower threshold, the interface generates a recovery alarm and restores to the normal state.

You can configure the input error packet alarm parameters in system view and interface view.

- The configuration in system view takes effect on all interfaces of the specified slot. The configuration in interface view takes effect only on the current interface.
- For an interface, the configuration in interface view takes priority, and the configuration in system view is used only when no configuration is made in interface view.

When you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the upper threshold to 5000, lower threshold to 400, and statistics collection and comparison interval to 6 seconds for input error packet alarms.

```
<Sysname> system-view
[Sysname] ifmonitor input-error slot 1 high-threshold 5000 low-threshold 400 interval 6
```

Related commands

snmp-agent trap enable ifmonitor

ifmonitor output-error

Use **ifmonitor output-error** to configure global output error packet alarm parameters.

Use **undo ifmonitor output-error** to restore the default.

NOTE:

This command is supported only in Release 6340 and later.

Syntax

ifmonitor output-error slot *slot-number* **high-threshold** *high-value* **low-threshold** *low-value* **interval** *interval* [**shutdown**]

undo ifmonitor output-error slot *slot-number*

Default

The upper threshold is 1000, the lower threshold is 100, and the statistics collection and comparison interval is 10 seconds for output error packet alarms.

Views

System view

Predefined user roles

network-admin

Parameters

high-threshold *high-value*: Specifies the upper threshold for output error packet alarms, in the range of 1 to 4294967295 packets.

low-threshold *low-value*: Specifies the lower threshold for output error packet alarms, in the range of 1 to 4294967295 packets.

interval *interval*: Specifies the statistics collection and comparison interval for output error packets, in the range of 1 to 65535 seconds.

shutdown: Shuts down an interface when the number of output error packets on the interface exceeds the upper threshold. Then, the interface stops forwarding all packets. To recover the interface, execute the **undo shutdown** command on the interface. If you do not specify this keyword, an upper threshold exceeding alarm is generated and the interface enters the alarm state when the number of output error packets exceeds the upper threshold on the interface.

slot *slot-number*: Specifies an IRF member device by its member ID.

Usage guidelines

With the output error packet alarm function enabled, when the number of output error packets on an interface in normal state within the specified interval exceeds the upper threshold, the interface generates an upper threshold exceeding alarm and enters the alarm state. When the number of

output error packets on an interface in the alarm state within the specified interval drops below the lower threshold, the interface generates a recovery alarm and restores to the normal state.

You can configure the output error packet alarm parameters in system view and interface view.

- The configuration in system view takes effect on all interfaces of the specified slot. The configuration in interface view takes effect only on the current interface.
- For an interface, the configuration in interface view takes priority, and the configuration in system view is used only when no configuration is made in interface view.

When you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the upper threshold to 5000, lower threshold to 400, and statistics collection and comparison interval to 6 seconds for output error packet alarms.

```
<Sysname> system-view
[Sysname] ifmonitor output-error slot 1 high-threshold 5000 low-threshold 400 interval
6
```

Related commands

snmp-agent trap enable ifmonitor

interface

Use **interface** to enter interface view.

Syntax

interface *interface-type interface-number*

Views

System view

Predefined user roles

network-admin

Parameters

interface-type: Specifies an interface type.

interface-number: Specifies an interface number.

Examples

Enter the view of GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1]
```

jumboframe enable

Use **jumboframe enable** to allow jumbo frames within the specified length to pass through.

Use **undo jumboframe enable** to prevent jumbo frames from passing through.

Use **undo jumboframe enable** *size* to restore the default.

Syntax

jumboframe enable [*size*]

undo jumboframe enable [*size*]

Default

The device allows jumbo frames within 10240 bytes to pass through.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

size: Sets the maximum length of (in bytes) Ethernet frames that are allowed to pass through. The value range for this argument is 1522 to 10240.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Allow jumbo frames to pass through GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] jumboframe enable
```

link-delay

Use **link-delay** to set the physical state change suppression interval on an Ethernet interface.

Use **undo link-delay** to restore the default.

Syntax

link-delay { **down** | **up** } [**msec**] *delay-time*

undo link-delay { **down** | **up** }

Default

Each time the physical link of a port goes up or comes down, the interface immediately reports the change to the CPU.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

down: Suppresses link-down events.

up: Suppresses link-up events.

msec: Enables the physical state change suppression interval to be accurate to milliseconds. If you do not specify this keyword, the suppression interval is accurate to seconds.

delay-time: Sets the physical state change suppression interval on the Ethernet interface. A value of 0 means that physical state changes are immediately reported to the CPU and are not suppressed.

- If you do not specify the **msec** keyword, the value range is 0 to 30 seconds.
- If you specify the **msec** keyword, the value range is 0 to 10000 milliseconds, and the value must be a multiple of 100.

Usage guidelines

You can configure this feature to suppress only link-down events, only link-up events, or both. If an event of the specified type still exists when the suppression interval expires, the system reports the event.

When you configure this feature, follow these guidelines:

- To suppress link-down events, configure the **link-delay down** command.
- To suppress link-up events, configure the **link-delay up** command.

On an interface, you can configure different suppression intervals for link-up and link-down events. If you execute the **link-delay** command multiple times on an interface, the following rules apply:

- You can configure the suppression intervals for link-up and link-down events separately.
- If you configure the suppression interval multiple times for link-up or link-down events, the most recent configuration takes effect.

Do not execute this command on an interface that has RRPP, spanning tree protocols, or Smart Link enabled. The S5000E-X, S5000X-EI, S5110V2-SI, S5000V3-EI, S5000V5-EI, and WAS6000 switches do not support RRPP or Smart Link.

This command, the **dampening** command, and the **port link-flap protect enable** command are mutually exclusive on an Ethernet interface.

Examples

Set the link-down event suppression interval to 8 seconds on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] link-delay down 8
```

Set the link-up event suppression interval to 800 milliseconds on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] link-delay up msec 800
```

Related commands

dampening

port link-flap protect enable

link-flap protect enable

Use **link-flap protect enable** to enable link flapping protection globally.

Use **undo link-flap protect enable** to disable link flapping protection globally.

Syntax

link-flap protect enable

undo link-flap protect enable

Default

Link flapping protection is disabled globally.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Link flapping on any interface changes network topology and increases the system overhead. For example, in an active/standby link scenario, when the interface status on the active link changes between **UP** and **DOWN**, traffic switches between active and standby links. To solve this problem, execute this command.

With link flapping protection enabled on an interface, when the interface goes down, the system enables link flapping detection on the interface. During the link flapping detection interval, if the number of detected flaps reaches or exceeds the link flapping detection threshold, the system shuts down the interface.

Link flapping protection takes effect only when it is enabled in both system view and interface view.

Examples

Enable link flapping protection globally.

```
<Sysname> system-view
[Sysname] link-flap protect enable
```

Related commands

port link-flap protect enable

loopback

Use **loopback** to enable loopback testing on an Ethernet interface.

Use **undo loopback** to disable loopback testing on an Ethernet interface.

Syntax

loopback { **external** | **internal** }

undo loopback

Default

Loopback testing is disabled on an Ethernet interface.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

external: Enables external loopback testing on the Ethernet interface.

internal: Enables internal loopback testing on the Ethernet interface.

Usage guidelines

An Ethernet interface in a loopback test cannot correctly forward data packets.

You cannot perform a loopback test on Ethernet interfaces manually brought down (displayed as in **ADM** or **Administratively DOWN** state).

The **speed**, **duplex**, and **shutdown** commands cannot be configured on an Ethernet interface in a loopback test.

The **shutdown**, **port up-mode**, and **loopback** commands are mutually exclusive.

Examples

Enable internal loopback testing on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] loopback internal
```

loopback-test

Use **loopback-test** to perform a loopback test.

NOTE:
This command is supported only in Release 6346 and later.

Syntax

loopback-test { **external** | **internal** }

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

external: Performs an external loopback test.

internal: Performs an internal loopback test.

Usage guidelines

The **shutdown**, **port up-mode**, **loopback**, and **loopback-test** commands are mutually exclusive on an interface.

Examples

Perform an internal loopback test on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] loopback-test internal
```

multicast-suppression

Use **multicast-suppression** to enable multicast storm suppression and set the multicast storm suppression threshold.

Use **undo multicast-suppression** to disable multicast storm suppression.

Syntax

multicast-suppression { *ratio* | **pps** *max-pps* | **kbps** *max-kbps* }

undo multicast-suppression

Default

Ethernet interfaces do not suppress multicast traffic.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

ratio: Sets the multicast suppression threshold as a percentage of the interface bandwidth. The value range for this argument (in percentage) is 0 to 100. A smaller value means that less multicast traffic is allowed to pass through.

pps *max-pps*: Specifies the maximum number of multicast packets that the interface can forward per second. The value range for the *max-pps* argument (in pps) is 0 to 1.4881 × the interface bandwidth.

kbps *max-kbps*: Specifies the maximum number of kilobits of multicast traffic that the Ethernet interface can forward per second. The value range for this argument (in kbps) is 0 to the interface bandwidth.

Usage guidelines

The multicast storm suppression feature limits the size of multicast traffic to a threshold on an interface. When the multicast traffic on the interface exceeds this threshold, the system drops packets until the traffic drops below this threshold.

Both the **storm-constrain** command and the **multicast-suppression** command can suppress multicast storms on a port. The **multicast-suppression** command uses the chip to physically suppress multicast traffic. It has less influence on the device performance than the **storm-constrain** command, which uses software to suppress multicast traffic.

For the traffic suppression result to be determined, do not configure both the **storm-constrain multicast** command and the **multicast-suppression** command on an interface.

When you configure the suppression threshold in kbps, the actual suppression threshold might be different from the configured one as follows:

- If the configured value is smaller than 64, the value of 64 takes effect.
- If the configured value is greater than 64 but not an integer multiple of 64, the integer multiple of 64 that is greater than and closest to the configured value takes effect.

To determine the suppression threshold that takes effect, see the prompts on the switch.

Examples

Set the multicast storm suppression threshold to 10000 kbps on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] multicast-suppression kbps 10000
The actual value is 10048 on port GigabitEthernet1/0/1 currently.
```

The output shows that the value that takes effect is 10048 kbps (157 times of 64), because the chip only supports step 64.

Related commands

broadcast-suppression

unicast-suppression

port auto-power-down

IMPORTANT:
Fiber ports do not support this command.

Use **port auto-power-down** to enable auto power-down on an Ethernet interface.

Use **undo port auto-power-down** to disable auto power-down on an Ethernet interface.

Syntax

port auto-power-down

undo port auto-power-down

Default

Auto power-down is disabled on Ethernet interfaces.

Views

Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

When an interface with auto power-down enabled has been down for a specific period of time, both of the following events occur:

- The device automatically stops supplying power to the interface.
- The interface enters the power save mode.

The time period depends on the chip specifications and is not configurable.

When the interface comes up, both of the following events occur:

- The device automatically restores the power supply to the interface.
- The interface restores to its normal state.

Examples

Enable auto power-down on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port auto-power-down
```

port ifmonitor crc-error

Use **port ifmonitor crc-error** to configure CRC error packet alarm parameters for an interface.

Use **undo port ifmonitor crc-error** to restore the default.

Syntax

port ifmonitor crc-error high-threshold *high-value* **low-threshold** *low-value* **interval** *interval* [**shutdown**]

undo port ifmonitor crc-error

NOTE:

This command is supported only in Release 6340 and later.

Default

An interface uses the global CRC error packet alarm parameters.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

high-threshold *high-value*: Specifies the upper threshold for CRC error packet alarms. If you specify the **ratio** keyword, the value range is 1 to 100. If you do not specify the **ratio** keyword, the value range is 1 to 4294967295 packets.

low-threshold *low-value*: Specifies the lower threshold for CRC error packet alarms. If you specify the **ratio** keyword, the value range is 1 to 100. If you do not specify the **ratio** keyword, the value range is 1 to 4294967295 packets.

interval *interval*: Specifies the statistics collection and comparison interval for CRC error packets, in the range of 1 to 65535 seconds.

shutdown: Shuts down an interface when the number of incoming CRC error packets on the interface exceeds the upper threshold. Then, the interface stops forwarding all packets. To recover the interface, execute the **undo shutdown** command on the interface. If you do not specify this keyword, an upper threshold exceeding alarm is generated and the interface enters the alarm state when the number of incoming CRC error packets exceeds the upper threshold on the interface.

Usage guidelines

With the CRC error packet alarm function enabled, when the number of incoming CRC error packets on an interface in normal state within the specified interval exceeds the upper threshold, the interface generates an upper threshold exceeding alarm and enters the alarm state. When the number of incoming CRC error packets on an interface in the alarm state within the specified interval drops below the lower threshold, the interface generates a recovery alarm and restores to the normal state.

You can configure the CRC error packet alarm parameters in system view and interface view.

- The configuration in system view takes effect on all interfaces of the specified slot. The configuration in interface view takes effect only on the current interface.
- For an interface, the configuration in interface view takes priority, and the configuration in system view is used only when no configuration is made in interface view.

When you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the upper threshold to 5000, lower threshold to 400, and statistics collection and comparison interval to 6 seconds for CRC error packet alarms on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port ifmonitor crc-error high-threshold 5000
low-threshold 400 interval 6
```

Related commands

snmp-agent trap enable ifmonitor

port ifmonitor input-error

Use **port ifmonitor input-error** to configure input error packet alarm parameters for an interface.

Use **undo port ifmonitor input-error** to restore the default.

Syntax

port ifmonitor input-error high-threshold *high-value* **low-threshold** *low-value* **interval** *interval* [**shutdown**]

undo port ifmonitor input-error

NOTE:

This command is supported only in Release 6342 and later.

Default

An interface uses the global input error packet alarm parameters.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

high-threshold *high-value*: Specifies the upper threshold for input error packet alarms, in the range of 1 to 4294967295 packets.

low-threshold *low-value*: Specifies the lower threshold for input error packet alarms, in the range of 1 to 4294967295 packets.

interval *interval*: Specifies the statistics collection and comparison interval for input error packets, in the range of 1 to 65535 seconds.

shutdown: Shuts down an interface when the number of input error packets on the interface exceeds the upper threshold. Then, the interface stops forwarding all packets. To recover the interface, execute the **undo shutdown** command on the interface. If you do not specify this keyword, an upper threshold exceeding alarm is generated and the interface enters the alarm state when the number of input error packets exceeds the upper threshold on the interface.

Usage guidelines

With the input error packet alarm function enabled, when the number of input error packets on an interface in normal state within the specified interval exceeds the upper threshold, the interface generates an upper threshold exceeding alarm and enters the alarm state. When the number of input error packets on an interface in the alarm state within the specified interval drops below the lower threshold, the interface generates a recovery alarm and restores to the normal state.

You can configure the input error packet alarm parameters in system view and interface view.

- The configuration in system view takes effect on all interfaces of the specified slot. The configuration in interface view takes effect only on the current interface.
- For an interface, the configuration in interface view takes priority, and the configuration in system view is used only when no configuration is made in interface view.

When you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the upper threshold to 5000, lower threshold to 400, and statistics collection and comparison interval to 6 seconds for input error packet alarms on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port ifmonitor input-error high-threshold 5000
low-threshold 400 interval 6
```

Related commands

snmp-agent trap enable ifmonitor

port ifmonitor output-error

Use **port ifmonitor output-error** to configure output error packet alarm parameters for an interface.

Use **undo port ifmonitor output-error** to restore the default.

NOTE:

This command is supported only in Release 6342 and later.

Syntax

port ifmonitor output-error high-threshold *high-value* **low-threshold** *low-value* **interval** *interval* [**shutdown**]

undo port ifmonitor output-error

Default

An interface uses the global output error packet alarm parameters.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

high-threshold *high-value*: Specifies the upper threshold for output error packet alarms, in the range of 1 to 4294967295 packets.

low-threshold *low-value*: Specifies the lower threshold for output error packet alarms, in the range of 1 to 4294967295 packets.

interval *interval*: Specifies the statistics collection and comparison interval for output error packets, in the range of 1 to 65535 seconds.

shutdown: Shuts down an interface when the number of output error packets on the interface exceeds the upper threshold. Then, the interface stops forwarding all packets. To recover the interface, execute the **undo shutdown** command on the interface. If you do not specify this keyword, an upper threshold exceeding alarm is generated and the interface enters the alarm state when the number of output error packets exceeds the upper threshold on the interface.

Usage guidelines

With the output error packet alarm function enabled, when the number of output error packets on an interface in normal state within the specified interval exceeds the upper threshold, the interface generates an upper threshold exceeding alarm and enters the alarm state. When the number of output error packets on an interface in the alarm state within the specified interval drops below the lower threshold, the interface generates a recovery alarm and restores to the normal state.

You can configure the output error packet alarm parameters in system view and interface view.

- The configuration in system view takes effect on all interfaces of the specified slot. The configuration in interface view takes effect only on the current interface.
- For an interface, the configuration in interface view takes priority, and the configuration in system view is used only when no configuration is made in interface view.

When you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the upper threshold to 5000, lower threshold to 400, and statistics collection and comparison interval to 6 seconds for output error packet alarms on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port ifmonitor output-error high-threshold 5000
low-threshold 400 interval 6
```

Related commands

snmp-agent trap enable ifmonitor

port link-flap protect enable

Use **port link-flap protect enable** to enable link flapping protection on an interface.

Use **undo port link-flap protect enable** to disable link flapping protection on an interface.

Syntax

port link-flap protect enable [**interval** *interval* | **threshold** *threshold*] *

undo port link-flap protect enable [**interval** | **threshold**]

Default

Link flapping protection is disabled on an interface.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

interval: Specifies the link flapping detection interval in seconds. The value range for this argument is 10 to 60. The default value for this argument is 10.

threshold: Specifies the link flapping detection threshold in the range of 5 to 10. The default value for this argument is 5.

Usage guidelines

Link flapping protection takes effect only when it is enabled in both system view and interface view.

If you do not specify the **interval** *interval* or **threshold** *threshold* option when you execute the **port link-flap protect enable** command, the command uses the default settings.

If you specify the **interval** or **threshold** keyword when you execute the **undo port link-flap protect enable** command, the command restores the default setting for the keyword.

With link flapping protection enabled on an interface, when the interface goes down, the system enables link flapping detection on the interface. During the link flapping detection interval, if the number of detected flaps reaches or exceeds the link flapping detection threshold, the system shuts down the interface.

To bring up an interface that has been shut down by link flapping protection, execute the **undo shutdown** command.

This command, the **dampening** command, and the **link-delay** command are mutually exclusive on an Ethernet interface.

Examples

Enable link flapping protection on an interface. Set the link flapping detection interval to 10 seconds, and set the link flapping detection threshold to 5.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet 1/0/1] port link-flap protect enable interval 10 threshold 5
```

Related commands

dampening

link-delay

link-flap protect enable

port up-mode

Use **port up-mode** to forcibly bring up a fiber Ethernet port.

Use **undo port up-mode** to restore the default.

Syntax

port up-mode

undo port up-mode

Default

A fiber Ethernet port is not forcibly brought up. The physical state of a fiber port depends on the physical state of the fibers.

Views

Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

This command forcibly brings up a fiber Ethernet port and enables the port to forward packets unidirectionally over a single link. In this way, transmission links are well utilized.

Copper ports and combo interfaces do not support this command. This command is supported only in Release 6312 and later.

This command is not supported on interfaces 1 through 24 on an S5024FV3-EI switch.

The **shutdown**, **port up-mode**, and **loopback** commands are mutually exclusive.

A fiber Ethernet port does not support this command if the port is shut down by a protocol or by using the **shutdown** command.

A fiber Ethernet port does not support this command if the port joins an aggregation group.

Examples

Forcibly bring up fiber port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port up-mode
```

reset counters interface

Use **reset counters interface** to clear the interface statistics.

Syntax

reset counters interface [*interface-type* [*interface-number*]]

Views

User view

Predefined user roles

network-admin

Parameters

interface-type: Specifies an interface type.

interface-number: Specifies an interface number.

Usage guidelines

Use this command to clear history statistics if you want to collect traffic statistics for a specific time period.

If you do not specify an interface type, this command clears statistics for all interfaces.

If you specify an interface type but do not specify an interface number, this command clears statistics for all interfaces of the specified type.

Examples

Clear the statistics for GigabitEthernet 1/0/1.

```
<Sysname> reset counters interface gigabitethernet 1/0/1
```

Related commands

display counters interface

display counters rate interface

display interface

reset ethernet statistics

Use **reset ethernet statistics** to clear the Ethernet module statistics.

Syntax

reset ethernet statistics [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number:* Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears statistics for all IRF member devices.

Examples

Clear the Ethernet module statistics for the specified slot.

```
<Sysname> reset ethernet statistics slot 1
```

Related commands

display ethernet statistics

shutdown

Use **shutdown** to shut down an Ethernet interface.

Use **undo shutdown** to bring up an Ethernet interface.

Syntax

shutdown

undo shutdown

Default

Ethernet interfaces are in up state.

Views

Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

CAUTION:
Executing the **shutdown** command on an interface will disconnect the link of the interface and interrupt communication. Use this command with caution.

Some interface configurations might require an interface restart before taking effect.

The **shutdown** command cannot be executed on an interface in a loopback test.

The **shutdown**, **port up-mode**, and **loopback** commands are mutually exclusive.

Examples

Shut down and then bring up GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] shutdown
[Sysname-GigabitEthernet1/0/1] undo shutdown
```

snmp-agent trap enable ifmonitor

Use **snmp-agent trap enable ifmonitor** to enable interface alarm functions.

Use **undo snmp-agent trap enable ifmonitor** to disable interface alarm functions.

NOTE:
This command is supported only in Release 6340 and later.

Syntax

snmp-agent trap enable ifmonitor [**crc-error** | **input-error** | **output-error**] *

undo snmp-agent trap enable ifmonitor [**crc-error** | **input-error** | **output-error**] *

Default

Interface alarm functions are enabled.

Views

System view

Predefined user roles

network-admin

Parameters

crc-error: Enables the CRC error packet alarm function for interfaces.

input-error: Enables the input error packet alarm function for interfaces.

output-error: Enables the output error packet alarm function for interfaces.

Examples

Enable the CRC error packet alarm function for interfaces.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable ifmonitor crc-error
```

speed

Use **speed** to set the speed of an Ethernet interface.

Use **undo speed** to restore the default.

Syntax

speed { **100** | **1000** | **2500** | **5000** | **10000** | **auto** }

undo speed

Default

An Ethernet interface negotiates a speed with its peer.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

10: Sets the interface speed to 10 Mbps.

100: Sets the interface speed to 100 Mbps.

1000: Sets the interface speed to 1000 Mbps.

2000: Sets the interface speed to 2000 Mbps.

2500: Sets the interface speed to 2500 Mbps.

5000: Sets the interface speed to 5000 Mbps.

10000: Sets the interface speed to 10000 Mbps.

auto: Enables the interface to negotiate a speed with its peer.

Usage guidelines

For an Ethernet copper port, use the **speed** command to set its speed to match the speed of the peer interface. Support of copper ports for keywords of this command varies by copper port type. For more information, use the **speed ?** command in interface view. If the system does not prompt that operation failed when you configure a speed for a copper port, the copper port supports this speed. Otherwise, the copper port does not support this speed.

For a fiber port, use the **speed** command to set its speed to match the rate of a transceiver module. Support of fiber ports for keywords of this command varies by fiber port type. For more information, use the **speed ?** command in interface view. If the system does not prompt that operation failed when you configure a speed for a fiber port, the fiber port supports this speed. Otherwise, the fiber port does not support this speed.

Additionally, you must select a speed for a fiber port according to the transceiver module installed to ensure that the transceiver module can be used properly. If the transceiver module installed in a fiber port does not support the speed for the fiber port, the transceiver module cannot be used. For example, if the transceiver module installed in an SFP+ fiber port is an SFP GE transceiver module and the **speed 10000** command is executed on the fiber port, the transceiver module can be used.

After a SFP-GE-T or SFP-GE-T-D transceiver module is installed in a fixed SFP port of the device, the port supports only the speed of 1000 Mbps. You can set the speed to 1000 Mbps by using the **speed** command or configure the port to autonegotiate the speed as 1000 Mbps by using the **speed auto** command.

Examples

Configure GigabitEthernet 1/0/1 to autonegotiate the speed.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] speed auto
```

Related commands

speed auto

speed auto downgrade

Use **speed auto downgrade** to enable automatic negotiation for speed downgrading.

Use **undo speed auto downgrade** to disable automatic negotiation for speed downgrading.

Syntax

speed auto downgrade

undo speed auto downgrade

Default

Automatic negotiation for speed downgrading is enabled.

Views

Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

This command takes effect after you configure it on the interface at either end of a link and the two interfaces are configured to automatically negotiate the speed.

This command is applicable only to GE interfaces.

Examples

Enable automatic negotiation for speed downgrading on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] speed auto downgrade
```

Related commands

speed auto

unicast-suppression

Use **unicast-suppression** to enable unknown unicast storm suppression and set the unknown unicast storm suppression threshold.

Use **undo unicast-suppression** to disable unknown unicast storm suppression.

Syntax

unicast-suppression { *ratio* | **pps** *max-pps* | **kbps** *max-kbps* }

undo unicast-suppression

Default

Ethernet interfaces do not suppress unknown unicast traffic.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

ratio: Sets the unknown unicast suppression threshold as a percentage of the interface bandwidth. The value range for this argument (in percentage) is 0 to 100. A smaller value means that less unknown unicast traffic is allowed to pass through.

pps *max-pps*: Specifies the maximum number of unknown unicast packets that the interface can forward per second. The value range for the *max-pps* argument (in pps) is 0 to 1.4881 × the interface bandwidth.

kbps *max-kbps*: Specifies the maximum number of kilobits of unknown unicast traffic that the Ethernet interface can forward per second. The value range for this argument (in kbps) is 0 to the interface bandwidth.

Usage guidelines

The unknown unicast storm suppression feature limits the size of unknown unicast traffic to a threshold on an interface. When the unknown unicast traffic on the interface exceeds this threshold, the system discards packets until the unknown unicast traffic drops below this threshold.

Both the **storm-constrain** command and the **unicast-suppression** command can suppress unknown unicast storms on a port. The **unicast-suppression** command uses the chip to physically suppress unknown unicast traffic. It has less influence on the device performance than the **storm-constrain** command, which uses software to suppress unknown unicast traffic.

For the unknown unicast traffic suppression result to be determined, do not configure both the **storm-constrain unicast** command and the **unicast-suppression** command on an interface.

When you configure the suppression threshold in kbps, the actual suppression threshold might be different from the configured one as follows:

- If the configured value is smaller than 64, the value of 64 takes effect.
- If the configured value is greater than 64 but not an integer multiple of 64, the integer multiple of 64 that is greater than and closest to the configured value takes effect.

To determine the suppression threshold that takes effect, see the prompts on the switch.

Examples

Set the unknown unicast storm suppression threshold to 10000 kbps on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] unicast-suppression kbps 10000
The actual value is 10048 on port GigabitEthernet1/0/1 currently.
```

The output shows that the value that takes effect is 10048 kbps (157 times of 64), because the chip only supports step 64.

Related commands

broadcast-suppression

multicast-suppression

Layer 2 Ethernet interface commands

display storm-constrain

Use **display storm-constrain** to display storm control settings and statistics.

Syntax

display storm-constrain [**broadcast** | **multicast** | **unicast**] [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

broadcast: Displays broadcast storm control settings and statistics.

multicast: Displays multicast storm control settings and statistics.

unicast: Displays unknown unicast storm control settings and statistics.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify this option, the command displays storm control settings and statistics for all storm control-enabled interfaces.

Usage guidelines

If you do not specify any keywords, this command displays all storm control settings on all storm control-enabled interfaces.

Examples

Display the storm control settings on all storm control-enabled ports.

```
<Sysname> display storm-constrain
```

```
 Abbreviation: BC - broadcast; MC - multicast; UC - unknown unicast;
               KNUC - known unicast; FW - forwarding
 Flow Statistic Interval: 5 (in seconds)
Port          Type Lower     Upper     Unit  Mode     Status   Trap Log StateChg
------------------------------------------------------------------------------
GE1/0/1       MC   100       200       kbps  shutdown shutdown off  on  10
```

Table 8 Command output

Field	Description
Flow Statistic Interval	Traffic polling interval (in seconds) of the storm control module.
Port	Abbreviated interface name.
Type	Type of traffic subjected to storm control: • **BC**—Broadcast packets. • **MC**—Multicast packets. • **UC**—Unknown unicast packets. • **KNUC**—Known unicast packets. This field is not supported in the current software version.
Lower	Lower storm control threshold, in pps, kbps, or percentage.
Upper	Upper storm control threshold, in pps, kbps, or percentage.
Unit	Storm control threshold unit: • pps. • kbps. • percentage.
Mode	Action (block or shutdown) taken on the interface when the upper threshold is reached. N/A indicates that no action is configured.
Status	Packet forwarding status: • **FW**—The port is forwarding traffic correctly. • **shutdown**—The port has been shut down. • **block**—The port drops the type of traffic.
Trap	Status of the storm control threshold event trap switch: • **on**—The port sends threshold event traps. • **off**—The port does not send threshold event traps.
Log	Status of the storm control threshold event log switch: • **on**—The port sends threshold event log messages. • **off**—The port does not send threshold event log messages.
StateChg	Number of forwarding state changes of the interface. When the **StateChg** field reaches 65535, it resets automatically.

display virtual-cable-test

Use **`display virtual-cable-test`** to display test results for the cable connected to an Ethernet interface.

IMPORTANT:

This command is supported only in Release 6350 and later versions.

Syntax

display virtual-cable-test interface [*interface-type interface-number* | *interface-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an Ethernet interface by its interface type and interface number. If you do not specify this parameter, the command displays test results for the cable connected to all Ethernet interfaces.

Usage guidelines

The test results are for reference only. The maximum error in length tested is 10 m (32.81 ft).

The test result is displayed as Invalid when the test cable length is in the range of 0 to 3 m (0 to 9.84 ft).

Fiber ports and interfaces operating at 10 Mbps or 100 Mbps and in up state do not support cable connection test.

When the local interface is shut down, cable connection test cannot be performed. When the peer interface is shut down, the length of the cable cannot be tested.

Examples

Display test results for the cable connected to all Ethernet interfaces.

```
<Sysname>display virtual-cable-test
Interface                   Result          Length(meters)      Date
GigabitEthernet1/0/1        Not test
GigabitEthernet1/0/2        Abnormal(open)  <50                 2013-03-06 23:01:34
```

Display test results for the cable connected to GigabitEthernet 1/0/2.

```
<Sysname> display virtual-cable-test interface GigabitEthernet 1/0/2
 Cable status:
  Pair A length: Invalid meters
  Pair B length: Invalid meters
  Pair C length: Invalid meters
  Pair D length: Invalid meters
  Pair A state: Abnormal(open)
  Pair B state: Abnormal(open)
  Pair C state: Abnormal(open)
  Pair D state: Abnormal(open)
Pair Impedance mismatch: no
Pair skew: - ns
Pair swap: -
Pair polarity: -
Insertion loss: - db
Return loss: - db
Near-end crosstalk: - db
```

Table 9 Command output

Field	Description
Interface	Name of the interface.
Result	Test results: • **Abnormal (open)**—An open circuit is detected. • **Abnormal (short)**—A short circuit is detected. • **Not test**—The test failed.
Length(meters)	Total length of the wire pair in meters.
Date	Time when the test was performed.
Pair x length	When the cable pair state is **OK**, this field displays the total length of the cable pair. When the cable pair is in any other state, this field displays the length from the local interface to the faulty point.
Pair x state	Cable pair state: • **OK**—The cable pair is in good condition. • **Abnormal**—The cable pair is abnormal. • **Abnormal (open)**—An open circuit is detected. • **Abnormal (short)**—A short circuit is detected. • **Invalid**—The test failed.
Pair Impedance mismatch	Pair impedance state: • **yes**—The pair impedance matches. • **no**—The pair impedance does not match.
Pair skew	If this field displays a hyphen (**-**), this field is not supported in the current software version.
Pair swap	If this field displays a hyphen (**-**), this field is not supported in the current software version.
Pair polarity	If this field displays a hyphen (**-**), this field is not supported in the current software version.
Insertion loss	If this field displays a hyphen (**-**), this field is not supported in the current software version.
Return loss	If this field displays a hyphen (**-**), this field is not supported in the current software version.
Near-end crosstalk	If this field displays a hyphen (**-**), this field is not supported in the current software version.

Related commands

`virtual-cable-test`

mdix-mode

IMPORTANT:

Fiber ports do not support this command.

Use **`mdix-mode`** to configure the Medium Dependent Interface Cross-Over (MDIX) mode of an Ethernet interface.

Use **`undo mdix-mode`** to restore the default.

Syntax

mdix-mode { **automdix** | **mdi**| **mdix** }

undo mdix-mode

Default

Ethernet interfaces operate in **automdix** mode.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

automdix: Specifies that the interface negotiates pin roles with its peer.

mdi: Specifies that pins 1 and 2 are transmit pins and pins 3 and 6 are receive pins.

mdix: Specifies that pins 1 and 2 are receive pins and pins 3 and 6 are transmit pins.

Examples

Configure GigabitEthernet 1/0/1 to operate in **automdix** mode.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mdix-mode automdix
```

port bridge enable

Use **port bridge enable** to enable bridging on an Ethernet interface.

Use **undo port bridge enable** to disable bridging on an Ethernet interface.

Syntax

port bridge enable

undo port bridge enable

Default

Bridging is disabled on an Ethernet interface.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

By default, the device drops packets whose outgoing interface and incoming interface are the same.

To enable the device to forward such packets rather than drop them, execute this command in Ethernet interface view. After the device receives a broadcast or unknown unicast packet, the device forwards the packet through all interfaces in the VLAN to which the incoming interface of the packet belongs.

Do not add interfaces configured with this command to an aggregation group.

Examples

Enable bridging on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port bridge enable
```

reset interface virtual-cable-test

Use **reset interface virtual-cable-test** to clear test results for the cable connected to an Ethernet interfaces.

IMPORTANT:
This command is supported only in Release 6350 and later versions.

Syntax

reset interface [*interface-type interface-number* | *interface-name*] **virtual-cable-test**

Views

User view

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an Ethernet interface by its type and number.

Examples

Clear test results for the cable connected to GigabitEthernet 1/0/1.

```
<Sysname> reset interface GigabitEthernet 1/0/1 virtual-cable-test
```

Related commands

virtual-cable-test

speed auto

Use **speed auto** to set options for speed autonegotiation.

Use **undo speed** to restore the default.

Syntax

speed auto { **10** | **100** | **1000** } *

undo speed

Default

No option is set for speed autonegotiation.

Views

100-Mbps or 1000-Mbps Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

10: Configures 10 Mbps as an option for speed autonegotiation.

100: Configures 100 Mbps as an option for speed autonegotiation.

1000: Configures 1000 Mbps as an option for speed autonegotiation.

Usage guidelines

The **speed** command and the **speed auto** command supersede each other. The most recent command that you configure takes effect. For example:

- If you configure **speed auto 100 1000** and then **speed 100** on the interface, the interface speed is forcibly set to 100 Mbps.
- If you configure **speed 100** and then **speed auto 100 1000** on the interface, the interface negotiates with its peer for a speed. The negotiated speed is either 100 Mbps or 1000 Mbps.

Speed autonegotiation enables an Ethernet interface to negotiate with its peer for the highest speed that both ends support. You can narrow down the speed option list for negotiation. To avoid negotiation failures, make sure a minimum of one speed option is supported at both ends.

Examples

Configure GigabitEthernet 1/0/1 to use 10 Mbps and 1000 Mbps for speed negotiation.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] speed auto 10 1000
```

Related commands

speed

storm-constrain

Use **storm-constrain** to enable storm control and set thresholds for broadcast, multicast, or unknown unicast packets on an Ethernet interface.

Use **undo storm-constrain** to disable storm control for broadcast, multicast, unknown unicast, or all types of traffic.

Syntax

storm-constrain { **broadcast** | **multicast** | **unicast** } { **pps** | **kbps** | **ratio** } *upperlimit lowerlimit*

undo storm-constrain { **all** | **broadcast** | **multicast** | **unicast** }

Default

Traffic storm control is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

all: Disables storm control for all types of traffic: broadcast, multicast, and unknown unicast.

broadcast: Enables or disables broadcast storm control.

multicast: Enables or disables multicast storm control.

unicast: Enables or disables unknown unicast storm control.

pps: Sets storm control thresholds in pps.

kbps: Sets storm control thresholds in kbps.

ratio: Sets storm control thresholds as a percentage of the transmission capacity of the interface.

upperlimit: Sets the upper threshold, in pps, kbps, or percentage.

- If you specify the **pps** keyword, the value range for the *upperlimit* argument is 0 to 1.4881 × the interface bandwidth.
- If you specify the **kbps** keyword, the value range for the *upperlimit* argument is 0 to the interface bandwidth.
- If you specify the **ratio** keyword, the value range for the *upperlimit* argument is 0 to 100.

lowerlimit: Sets the lower threshold, in pps, kbps, or percentage.

- If you specify the **pps** keyword, the value range for the *lowerlimit* argument is 0 to 1.4881 × the interface bandwidth.
- If you specify the **kbps** keyword, the value range for the *lowerlimit* argument is 0 to the interface bandwidth.
- If you specify the **ratio** keyword, the value range for the *lowerlimit* argument is 0 to 100.

Usage guidelines

After you configure storm control for a type of traffic, the device collects the statistics for the type of traffic at the interval configured by using the **storm-constrain interval** command. When the type of traffic exceeds its upper threshold, the interface takes an action configured by using the **storm-constrain control** command.

The **storm-constrain**, **broadcast-suppression**, **multicast-suppression**, and **unicast-suppression** commands can suppress storms on an interface. The **broadcast-suppression**, **multicast-suppression**, and **unicast-suppression** commands use the chip to physically suppress traffic. They have less influence on the device performance than the **storm-constrain** command, which uses software to suppress traffic.

For the traffic suppression result to be determined, do not configure both storm control and storm suppression for the same type of traffic.

When configuring this command, make sure *upperlimit* is greater than *lowerlimit*.

Examples

Enable unknown unicast storm control on GigabitEthernet 1/0/1 and set the upper and lower thresholds to 200 pps and 150 pps, respectively.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] storm-constrain unicast pps 200 150
```

Enable broadcast storm control on GigabitEthernet 1/0/2, and set the upper and lower thresholds to 2000 kbps and 1500 kbps, respectively.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] storm-constrain broadcast kbps 2000 1500
```

Enable multicast storm control on GigabitEthernet 1/0/3, and set the upper and lower thresholds to 80% and 15%, respectively.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/3
[Sysname-GigabitEthernet1/0/3] storm-constrain multicast ratio 80 15
```

Related commands

storm-constrain control

storm-constrain interval

storm-constrain control

Use **storm-constrain control** to set the action to take on an Ethernet interface when a type of traffic (unknown unicast, multicast, or broadcast) exceeds the upper storm control threshold.

Use **undo storm-constrain control** to restore the default.

Syntax

storm-constrain control { **block** | **shutdown** }

undo storm-constrain control

Default

No action is taken on an Ethernet interface when a type of traffic exceeds the upper storm control threshold.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

block: Blocks this type of traffic and forwards other types of traffic. Even though the interface does not forward the blocked traffic, it still counts the traffic. When the blocked traffic drops below the lower threshold, the port begins to forward the traffic.

shutdown: Goes down automatically. The interface goes down automatically and stops forwarding any traffic. When the blocked traffic drops below the lower threshold, the interface does not forward the traffic. To bring up the interface, use the **undo shutdown** command or disable storm control on the interface.

Examples

Configure GigabitEthernet 1/0/1 to block a specific type of traffic when the type of traffic exceeds the upper storm control threshold.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] storm-constrain control block
```

Related commands

storm-constrain

storm-constrain control

storm-constrain enable log

Use **storm-constrain enable log** to enable an Ethernet interface to output log messages when it detects storm control threshold events.

Use **undo storm-constrain enable log** to disable an Ethernet interface from outputting log messages for storm control threshold events.

Syntax

storm-constrain enable log

undo storm-constrain enable log

Default

An Ethernet interface outputs log messages when monitored traffic exceeds the upper threshold or drops below the lower threshold from a value above the upper threshold.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Examples

Enable GigabitEthernet 1/0/1 to output log messages when it detects storm control threshold events.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] storm-constrain enable log
```

storm-constrain enable trap

Use **storm-constrain enable trap** to enable an Ethernet interface to send storm control threshold event traps.

Use **undo storm-constrain enable trap** to disable an Ethernet interface from sending storm control threshold event traps.

Syntax

storm-constrain enable trap

undo storm-constrain enable trap

Default

An interface sends out storm control threshold event traps when monitored traffic exceeds the upper threshold or drops below the lower threshold from a value above the upper threshold.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Examples

Enable GigabitEthernet 1/0/1 to send traps when it detects storm control threshold events.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] storm-constrain enable trap
```

storm-constrain interval

Use **storm-constrain interval** to set the traffic polling interval of the storm control module.

Use **undo storm-constrain interval** to restore the default.

Syntax

storm-constrain interval *interval*

undo storm-constrain interval

Default

The storm control module polls traffic statistics every 10 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Sets the traffic polling interval of the storm control module. The value range is 1 to 300 seconds. To ensure network stability, as a best practice, do not use a traffic polling interval shorter than 10 seconds.

Usage guidelines

The traffic polling interval set by using the **storm-constrain interval** command is specific to storm control. To set the statistics polling interval of an interface, use the **flow-interval** command.

Examples

Set the traffic statistics polling interval of the storm control module to 60 seconds.

```
<Sysname> system-view
[Sysname] storm-constrain interval 60
```

Related commands

storm-constrain

storm-constrain control

virtual-cable-test

Use **virtual-cable-test** to test the cable connection of an Ethernet interface and display the test result.

Syntax

virtual-cable-test interface [*interface-type interface-number* | *interface-name*]

Views

Any view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an Ethernet interface by its type and number.

IMPORTANT:

This command is supported only in Release 6350 and later versions.

Usage guidelines

This command is not available on fiber ports.

If the link of an Ethernet interface is up, testing its cable connection will cause the link to go down and then up.

The test result is for reference only. The cable length detection error is up to 5 m (about 16 ft).

If a test item is not available, a hyphen (-) is displayed.

Examples

Test the cable connection of GigabitEthernet 1/0/1. (Available in version earlier than Release 6328.)

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] virtual-cable-test
Cable status: abnormal(open), 140 metre(s)
Pair Impedance mismatch: -
Pair skew: - ns
Pair swap: -
Pair polarity: -
Insertion loss: - db
Return loss: - db
Near-end crosstalk: - db
```

Test the cable connection of GigabitEthernet 1/0/1. (Available in Release 6328 and later.)

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] virtual-cable-test
Cable status:
  Pair A length: 1 meters
  Pair B length: 5 meters
  Pair C length: 1 meters
  Pair D length: 1 meters
  Pair A state: Abnormal(open)
  Pair B state: Abnormal(open)
  Pair C state: Abnormal(open)
  Pair D state: Abnormal(open)
Pair Impedance mismatch: yes
Pair skew: - ns
Pair swap: -
Pair polarity: -
Insertion loss: - db
Return loss: - db
Near-end crosstalk: - db
```

Table 10 Command output

Field	Description
Cable status (Available in version earlier than Release 6328.)	Cable status: • **Normal**—The cable is in good condition. • **Abnormal**—The cable is abnormal. • **Abnormal (open)**—An open circuit is detected.

Field	Description
	• **Abnormal (short)**—A short circuit is detected. • **Failure**—The test failed.
n metre(s) (Available in version earlier than Release 6328.)	If the cable connection is working correctly, this field displays the total length of the cable. If the cable connection fails, this field displays the length from the local port to the faulty point.
Pair *x* length (Available in Release 6328 and later.)	When the cable pair state is **OK**, this field displays the total length of the cable pair. When the cable pair is in any other state, this field displays the length from the local interface to the faulty point.
Pair x state (Available in Release 6328 and later.)	Cable pair state: • **OK**—The cable pair is in good condition. • **Abnormal**—The cable pair is abnormal. • **Abnormal (open)**—An open circuit is detected. • **Abnormal (short)**—A short circuit is detected. • **Invalid**—The test failed.

Contents

Loopback, null, and inloopback interface commands

bandwidth

Use **bandwidth** to set the expected bandwidth for an interface.

Use **undo bandwidth** to restore the default.

Syntax

bandwidth *bandwidth-value*

undo bandwidth

Default

The expected bandwidth of a loopback interface is 0 kbps.

Views

Loopback interface view

Predefined user roles

network-admin

Parameters

bandwidth-value: Specifies the expected bandwidth in the range of 1 to 400000000 kbps.

Usage guidelines

The expected bandwidth is an informational parameter used only by higher-layer protocols for calculation. You cannot adjust the actual bandwidth of an interface by using this command.

Examples

Set the expected bandwidth of Loopback 1 to 1000 kbps.

```
<Sysname> system-view
[Sysname] interface loopback 1
[Sysname-LoopBack1] bandwidth 1000
```

default

Use **default** to restore the default settings for an interface.

Syntax

default

Views

Loopback interface view

Null interface view

Predefined user roles

network-admin

Usage guidelines

CAUTION:

The **default** command might interrupt ongoing network services. Make sure you are fully aware of the impact of this command before using it on a live network.

This command might fail to restore the default settings for some commands for reasons such as command dependencies and system restrictions. Use the **display this** command in interface view to identify these commands, and then use their **undo** forms or follow the command reference to restore their default settings. If your restoration attempt still fails, follow the error message instructions to resolve the problem.

Examples

Restore the default settings for Loopback 1.

```
<Sysname> system-view
[Sysname] interface loopback 1
[Sysname-LoopBack1] default
```

description

Use **description** to configure the description of an interface.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

The interface description uses the *interface name* **Interface** format, for example, LoopBack1 **Interface**.

Views

Loopback interface view

Null interface view

Predefined user roles

network-admin

Parameters

text: Specifies the description, a case-sensitive string of 1 to 255 characters.

Usage guidelines

Configure a description for an interface for easy identification and management purposes.

You can use the **display interface** command to view the configured description.

Examples

Configure the description of Loopback 1 as **for RouterID**.

```
<Sysname> system-view
[Sysname] interface loopback 1
[Sysname-LoopBack1] description for RouterID
```

display interface inloopback

Use **display interface inloopback** to display information about the inloopback interface.

Syntax

display interface [**inloopback** [**0**]] [**brief** [**description** | **down**]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

inloopback [**0**]: Specifies Inloopback 0. If you do not specify the **inloopback** keyword, the command displays information about all interfaces.

brief: Displays brief interface information. If you do not specify this keyword, the command displays detailed interface information.

description: Displays complete interface descriptions. If you do not specify this keyword, the command displays only the first 27 characters of interface descriptions. The description of an inloopback interface is always **InLoopBack0 Interface** and cannot be configured.

down: Displays information about interfaces in down state and the causes. If you do not specify this keyword, the command displays information about interfaces in all states.

Usage guidelines

The device has only one inloopback interface Inloopback 0. If you specify the **inloopback** keyword, the command displays information about the interface Inloopback 0 regardless of whether you specify the **0** keyword.

Examples

Display detailed information about Inloopback 0.

```
<Sysname> display interface inloopback
InLoopBack0
Current state: UP
Line protocol state: UP(spoofing)
Description: InLoopBack0 Interface
Maximum transmission unit: 1536
Physical: InLoopBack
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

Table 1 Command output

Field	Description
Current state	Physical link state of the interface, which is always **UP**, meaning that the inloopback interface can receive and transmit packets.

Field	Description
Line protocol state	Data link layer state of the interface, which is always **UP(spoofing)**. **UP(spoofing)** represents that the data link layer protocol of the interface is up, but the link is an on-demand link or does not exist. This attribute is typical of null interfaces and loopback interfaces.
Description	Description of the interface, which is always **InLoopBack0 Interface** and cannot be configured.
Maximum transmission unit	MTU of the interface, which is always 1536 and cannot be configured
Physical: InLoopBack	The physical type of the interface is inloopback.
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	Average input rate during the last 300 seconds (displayed when the interface supports traffic statistics collection): • **bytes/sec**—Average number of bytes received per second. • **bits/sec**—Average number of bits received per second. • **packets/sec**—Average number of packets received per second.
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	Average output rate over the last 300 seconds (displayed when the interface supports traffic statistics collection): • **bytes/sec**—Average number of bytes sent per second. • **bits/sec**—Average number of bits sent per second. • **packets/sec**—Average number of packets sent per second.
Input: 0 packets, 0 bytes, 0 drops	Total number and size (in bytes) of incoming packets of the interface and the number of dropped packets (displayed when the interface supports traffic statistics collection).
Output: 0 packets, 0 bytes, 0 drops	Total number and size (in bytes) of outgoing packets of the interface and the number of dropped packets (displayed when the interface supports traffic statistics collection).

Display brief information about Inloopback 0.

```
<Sysname> display interface inloopback 0 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP         Description
InLoop0              UP   UP(s)    --
```

Table 2 Command output

Field	Description
Link	Physical link state of the interface, which is always **UP**, meaning that the link is physically up.
Protocol	Data link layer protocol state of the interface, which is always **UP(s)**. **UP(s)** represents that the data link layer protocol of the interface is up, but the link is an on-demand link or does not exist. The **(s)** attribute represents the spoofing flag. This value is typical of null interfaces and loopback interfaces.
Primary IP	IP address of the interface. Because inloopback interfaces do not support CLI configuration, this field does not display a value.

Field	Description
Description	Description of the interface. Because inloopback interfaces do not support CLI configuration, this field does not display a value.

display interface loopback

Use **display interface loopback** to display information about the specified or all existing loopback interfaces.

Syntax

display interface [**loopback** [*interface-number*]] [**brief** [**description** | **down**]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

loopback *interface-number*: Specifies a loopback interface by its number, which can be the number of any existing loopback interface. If you do not specify the **loopback** keyword, the command displays information about all interfaces. If you specify the **loopback** keyword but do not specify the *interface-number* argument, the command displays information about all existing loopback interfaces on the device.

brief: Displays brief interface information. If you do not specify this keyword, the command displays detailed interface information.

description: Displays complete interface descriptions. If you do not specify this keyword, the command displays only the first 27 characters of interface descriptions.

down: Displays information about interfaces in down state and the causes. If you do not specify this keyword, the command displays information about interfaces in all states.

Usage guidelines

This command is supported only after a loopback interface is created.

Examples

Display detailed information about Loopback 0.

```
<Sysname> display interface loopback 0
LoopBack0
Current state: UP
Line protocol state: UP(spoofing)
Description: LoopBack0 Interface
Bandwidth: 1000 kbps
Maximum transmission unit: 1536
Internet protocol processing: Disabled
Physical: Loopback
Last clearing of counters:  Never
```

```
Last 300 seconds input rate:  0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate:  0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

Table 3 Command output

Field	Description
Current state	Physical link state of the interface: • **UP**—The loopback interface can receive and transmit packets. • **Administratively DOWN**—The interface has been shut down by using the **shutdown** command.
Line protocol state	Data link layer state of the interface. **UP (spoofing)** means that the data link layer protocol of the interface is up, but the link is an on-demand link or does not exist. This attribute is typical of null interfaces and loopback interfaces.
Description	Description of the interface.
Bandwidth	Expected bandwidth of the interface. This field is not displayed when the value is 0.
Maximum transmission unit	MTU of the interface.
Internet protocol processing: Disabled	The interface is not assigned an IP address and cannot process IP packets.
Internet address: 1.1.1.1/32 (primary)	IP address of the interface. The **primary** attribute indicates that the address is the primary IP address.
Physical: Loopback	The physical type of the interface is loopback.
baudrate	Baud rate, in Kbps.
Last clearing of counters	Time when statistics on the logical interface were last cleared by using the **reset counters interface** command. If the statistics of the interface have never been cleared by using the **reset counters interface** command since the device started, this field displays **Never**.
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	Average input rate during the last 300 seconds (displayed when the interface supports traffic statistics collection): **bytes/sec**—Average number of bytes received per second. **bits/sec**—Average number of bits received per second. **packets/sec**—Average number of packets received per second.
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	Average output rate over the last 300 seconds (displayed when the interface supports traffic statistics collection): • **bytes/sec**—Average number of bytes sent per second. • **bits/sec**—Average number of bits sent per second. • **packets/sec**—Average number of packets sent per second.
Input: 0 packets, 0 bytes, 0 drops	Total number and size (in bytes) of incoming packets of the interface and the number of dropped packets (displayed when the interface supports traffic statistics collection).
Output: 0 packets, 0 bytes, 0 drops	Total number and size (in bytes) of outgoing packets of the interface and the number of dropped packets (displayed when the interface supports traffic statistics collection).

Display brief information about all loopback interfaces.

```
<Sysname> display interface loopback brief
```

```
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP         Description
Loop1                UP   UP(s)    --              forLAN1
```

Display information about all loopback interfaces in down state and the causes.

```
<Sysname> display interface loopback brief down
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Interface            Link Cause
Loop1                ADM  Administratively
```

Table 4 Command output

Field	Description
Link	Physical link state of the interface: • **UP**—The interface is physically up. • **DOWN**—The interface is physically down. • **ADM**—The interface has been shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **Stby**—The interface is a backup interface in standby state.
Protocol	Data link layer protocol state of the interface, which is always **UP(s)**. **UP(s)** represents that the data link layer protocol of the interface is up, but the link is an on-demand link or does not exist. The **(s)** attribute represents the spoofing flag. This value is typical of null interfaces and loopback interfaces.
Primary IP	Primary IP address of the interface.
Description	Description of the interface.
Cause	Cause for the physical link state of the interface to be **DOWN**. **Administratively** represents that the interface has been manually shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command.

Related commands

interface loopback

reset counters interface loopback

display interface null

Use **display interface null** to display information about the null interface.

Syntax

display interface [**null** [**0**]] [**brief** [**description** | **down**]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

null [**0**]: Specifies Null 0. If you do not specify the **null** keyword, the command displays information about all interfaces.

brief: Displays brief interface information. If you do not specify this keyword, the command displays detailed interface information.

description: Displays complete interface descriptions. If you do not specify this keyword, the command displays only the first 27 characters of interface descriptions.

down: Displays information about interfaces in down state and the causes. If you do not specify this keyword, the command displays information about interfaces in all states.

Usage guidelines

The device has only one null interface Null 0. If you specify the **null** keyword, the command displays information about the interface Null 0 regardless of whether you specify the **0** keyword.

Examples

Display detailed information about Null 0.

```
<Sysname> display interface null 0
NULL0
Current state: UP
Line protocol state: UP(spoofing)
Description: NULL0 Interface
Bandwidth: 1000000 kbps
Maximum transmission unit: 1500
Internet protocol processing: Disabled
Physical: NULL DEV, baudrate: 1000000 kbps
Last clearing of counters: Never
Last 300 seconds input rate:  0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate:  0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

Display brief information about Null 0.

```
<Sysname> display interface null 0 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP         Description
NULL0                UP   UP(s)    --
```

For the command output, see Table 3 and Table 4.

Related commands

interface null

reset counters interface null

interface loopback

Use **interface loopback** to create a loopback interface and enter its view, or enter the view of an existing loopback interface.

Use **undo interface loopback** to remove a loopback interface.

Syntax

interface loopback *interface-number*

undo interface loopback *interface-number*

Default

No loopback interfaces exist.

Views

System view

Predefined user roles

network-admin

Parameters

interface-number: Specifies a loopback interface by its number. The value range for this argument is 0 to 127.

Usage guidelines

The physical layer state and link layer protocols of a loopback interface are always up unless the loopback interface is manually shut down. You can use a loopback interface to achieve the following purposes:

- Prevent the connection from being affected by the physical state of the interface.
- Improve the reliability of the connection.

For example, you can configure a loopback interface as the source interface for establishing an FTP connection.

Examples

Create Loopback 1.

```
<Sysname> system-view
[Sysname] interface loopback 1
[Sysname-LoopBack1]
```

interface null

Use **interface null** to enter null interface view.

Syntax

interface null 0

Default

A device has only one null interface (Null 0), which cannot be created or deleted.

Views

System view

Predefined user roles

network-admin

Parameters

0: Specifies Null 0. The null interface number is always 0.

Examples

Enter Null 0 interface view.

```
<Sysname> system-view
[Sysname] interface null 0
[Sysname-NULL0]
```

reset counters interface loopback

Use **reset counters interface loopback** to clear the statistics on the specified or all loopback interfaces.

Syntax

reset counters interface [**loopback** [*interface-number*]]

Views

User view

Predefined user roles

network-admin

Parameters

loopback [*interface-number*]: Specifies a loopback interface by its number, which can be the number of any existing loopback interface. If you do not specify the **loopback** keyword, the command clears the statistics on all interfaces. If you specify the **loopback** keyword but do not specify the *interface-number* argument, the command clears the statistics on all loopback interfaces.

Usage guidelines

To determine whether a loopback interface works correctly within a period by collecting the traffic statistics within that period, first use the **reset counters interface** [**loopback** [*interface-number*]] command to clear the statistics. Then have the interface automatically collect the statistics.

This command is available only if a minimum of one loopback interface has been created.

Examples

Clear the statistics on Loopback 1.

```
<Sysname> reset counters interface loopback 1
```

Related commands

display interface loopback

reset counters interface null

Use **reset counters interface null** to clear the statistics on the null interface.

Syntax

reset counters interface [**null** [**0**]]

Views

User view

Predefined user roles

network-admin

Parameters

null [**0**]: Specifies Null 0. If you do not specify the **null** keyword, the command clears the statistics on all interfaces.

Usage guidelines

To determine whether the null interface works correctly within a period by collecting the traffic statistics within that period, first use the **reset counters interface** [**null** [**0**]] command to clear the statistics. Then have the interface automatically collect the statistics.

Examples

Clear the statistics on Null 0.

```
<Sysname> reset counters interface null 0
```

Related commands

display interface null

shutdown

Use **shutdown** to shut down a loopback interface.

Use **undo shutdown** to bring up a loopback interface.

Syntax

shutdown

undo shutdown

Default

A loopback interface is up.

Views

Loopback interface view

Predefined user roles

network-admin

Usage guidelines

Use the **shutdown** command with caution, because the command disconnects the connection of the interface and disables the interface from communicating.

Examples

Shut down Loopback 1.

```
<Sysname> system-view
[Sysname] interface loopback 1
[Sysname-LoopBack1] shutdown
```

Contents

Bulk interface configuration commands

display interface range

Use **display interface range** to display information about named interface ranges created by using the **interface range name** command.

Syntax

display interface range [**name** *name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *name*: Specifies an interface range by its name, a case-sensitive string of 1 to 32 characters. If you do not specify an interface range name, this command displays information about all interface ranges created by using the **interface range name** command.

Examples

Display information about the interface ranges created by using the **interface range name** command.

```
<Sysname> display interface range
Interface range name t2 GigabitEthernet1/0/1 GigabitEthernet1/0/2
Interface range name test GigabitEthernet1/0/3 GigabitEthernet1/0/4
```

The output shows the following:

- Interfaces GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 are added to interface range **t2**.
- Interfaces GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 are added to interface range **test**.

Related commands

interface range name

interface range

Use **interface range** to create an interface range and enter the interface range view.

Syntax

interface range *interface-list*

Views

System view

Predefined user roles

network-admin

Parameters

interface-list: Specifies a space-separated list of up to 24 interface items. Each item specifies an interface by its type and number or specifies a subrange of interfaces in the form of

interface-type interface-number1 **to** *interface-type interface-number2*.When you specify a subrange of interfaces, the interfaces must be all fixed interfaces or on the same interface card. The start interface number must be identical to or lower than the end interface number.

Usage guidelines

Use this command to bulk configure multiple interfaces with the same feature instead of configuring them one by one. For example, execute the **shutdown** command in interface range view to shut down a range of interfaces.

The interface range created by using this command is not saved to the running configuration. You cannot use the interface range repeatedly. To create an interface range that can be used repeatedly, use the **interface range name** command.

In interface range view, only the commands supported by the first interface in the specified interface list (alphabetically sorted) are available for configuration. To view available commands, enter a question mark (?) in interface range view.

After a command is executed in interface range view, one of the following situations might occur:

- The system displays an error message and stays in interface range view. It means that the execution failed on one or multiple member interfaces.
  - If the execution failed on the first member interface, the command is not executed on any member interfaces.
  - If the execution failed on a non-first member interface, the command takes effect on the remaining member interfaces.
- The system returns to system view. It means that:
  - The command is supported in both system view and interface view.
  - The execution failed on a member interface in interface range view and succeeded in system view.
  - The command is not executed on the subsequent member interfaces.

  You can use the **display this** command to verify the configuration in interface view of each member interface. In addition, if the configuration in system view is not needed, use the **undo** form of the command to remove the configuration.

To verify the configuration of the first member interface, you can execute the **display this** command in interface range view.

The device does not output prompt or alarm messages during the bulk interface configuration process. Make sure you are fully aware of the impacts of the bulk interface configuration.

When you bulk configure interfaces, follow these guidelines:

- Before you configure an interface as the first interface in an interface range, make sure you can enter the view of the interface by using the **interface** *interface-type interface-number* command.
- Do not assign both an aggregate interface and any of its member interfaces to an interface range. Some commands, after being executed on both an aggregate interface and its member interfaces, can break up the aggregation.
- Understand that the more interfaces you specify, the longer the command execution time.

Examples

Shut down interfaces GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5.

```
<Sysname> system-view
[Sysname] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/5
[Sysname-if-range] shutdown
```

interface range name

Use **interface range name** *name* **interface** *interface-list* to create a named interface range and enter the interface range view.

Use **interface range name** *name* without the **interface** keyword to enter the view of a named interface range.

Use **undo interface range name** to delete the interface range with the specified name.

Syntax

interface range name *name* [**interface** *interface-list*]

undo interface range name *name*

Views

System view

Predefined user roles

network-admin

Parameters

name: Specifies an interface range name, a case-sensitive string of 1 to 32 characters.

interface-list: Specifies a space-separated list of up to 24 interface items. Each item specifies an interface by its type and number or a subrange of interfaces in the form of *interface-type interface-number1* **to** *interface-type interface-number2*.When you specify a subrange of interfaces, the interfaces must be all fixed interfaces or on the same interface card. The start interface number must be identical to or lower than the end interface number.

Usage guidelines

A named interface range is saved in the running configuration and can be used repeatedly to bulk configure its member interfaces.

In interface range view, only the commands supported by the first interface in the specified interface list (alphabetically sorted) are available for configuration. To view available commands, enter a question mark (?) in interface range view.

After a command is executed in interface range view, one of the following situations might occur:

- The system displays an error message and stays in interface range view. It means that the execution failed on one or multiple member interfaces.
  - If the execution failed on the first member interface, the command is not executed on any member interfaces.
  - If the execution failed on a non-first member interface, the command takes effect on the remaining member interfaces.
- The system returns to system view. It means that:
  - The command is supported in both system view and interface view.
  - The execution failed on a member interface in interface range view and succeeded in system view.
  - The command is not executed on the subsequent member interfaces.

  You can use the **display this** command to verify the configuration in interface view of each member interface. In addition, if the configuration in system view is not needed, use the **undo** form of the command to remove the configuration.

To verify the configuration of the first interface, you can execute the **display this** command in interface range view.

To view the member interfaces of a named interface range, use the **display interface range** command.

The device does not output prompt or alarm messages during the bulk interface configuration process. Make sure you are fully aware of the impacts of the bulk interface configuration.

When you bulk configure interfaces, follow these guidelines:

- Before you configure an interface as the first interface in an interface range, make sure you can enter the view of the interface by using the **interface** *interface-type interface-number* command.
- Do not assign both an aggregate interface and any of its member interfaces to an interface range. Some commands, after being executed on both an aggregate interface and its member interfaces, can break up the aggregation.
- Understand that the more interfaces you specify, the longer the command execution time.
- To guarantee bulk interface configuration performance, configure fewer than 1000 interface range names.

Examples

Add GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5 to interface range **myEthPort**, and enter the interface range view.

```
<Sysname> system-view
[Sysname] interface range name myEthPort interface gigabitethernet 1/0/1 to
gigabitethernet 1/0/5
[Sysname-if-range-myEthPort]
```

Enter the view of interface range **myEthPort**.

```
<Sysname> system-view
[Sysname] interface range name myEthPort
[Sysname-if-range-myEthPort]
```

Related commands

display interface range

Contents

MAC address table commands

This document covers the configuration of unicast MAC address entries, including static, dynamic, blackhole, and multiport unicast MAC address entries. For more information about configuring static multicast MAC address entries, see IGMP snooping and IPv6 multicast routing and forwarding in *IP Multicast Configuration Guide*.

display mac-address

Use **display mac-address** to display MAC address entries.

Syntax

display mac-address [*mac-address* [**vlan** *vlan-id*] | [[**dynamic** | **static**] [**interface** *interface-type interface-number*] | **blackhole** | **multiport**] [**vlan** *vlan-id*] [**count**]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

mac-address: Specifies a MAC address in the format of H-H-H. When entering a MAC address, you can omit the leading zeros in each H section. For example, enter f-e2-1 for 000f-00e2-0001.

vlan *vlan-id*: Specifies a VLAN by its ID in the range of 1 to 4094.

dynamic: Displays dynamic MAC address entries.

static: Displays static MAC address entries.

interface *interface-type interface-number*: Specifies an interface by its type and number.

blackhole: Displays blackhole MAC address entries.

multiport: Displays multiport unicast MAC address entries.

count: Displays only the number of MAC address entries that match all entry attributes you specify in the command. Detailed information about MAC address entries is not displayed. For example, you can use the **display mac-address vlan 20 dynamic count** command to display the number of dynamic entries for VLAN 20. If you do not specify an entry attribute, the command displays the number of entries in the MAC address table. If you do not specify this keyword, the command displays detailed information about the specified MAC address entries.

Usage guidelines

A MAC address entry includes a destination MAC address, an outgoing interface, and a VLAN ID.

If you do not specify any parameters, the command displays all MAC address entries.

This command displays dynamic MAC address entries for an aggregate interface only when the aggregate interface has a minimum of one Selected member port.

Multiport unicast MAC address entries have no impact on the MAC address learning. When receiving a frame whose source MAC address matches a multiport unicast entry, the device can still learn the MAC address of the frame and generate a dynamic entry. However, the generated dynamic

entry has lower priority. The device prefers to use the multiport unicast entry to forward frames destined for the MAC address in the entry.

Examples

Display MAC address entries for VLAN 100.

```
<Sysname> display mac-address vlan 100
MAC Address      VLAN ID    State           Port/Nickname           Aging
0001-0101-0101   100        Multiport       GE1/0/1                 N
                                            GE1/0/2
0033-0033-0033   100        Blackhole       N/A                     N
0000-0000-0002   100        Static          GE1/0/3                 N
00e0-fc00-5829   100        Learned         GE1/0/4                 Y
```

Display the number of MAC address entries.

```
<Sysname> display mac-address count
1 mac address(es) found.
```

Table 1 Command output

Field	Description
VLAN ID	ID of the VLAN to which the outgoing interface of the MAC address entry belongs.
State	MAC address entry state: • **Static**—Static MAC address entry. • **Learned**—Dynamic MAC address entry. Dynamic entries can be learned or manually configured. • **Blackhole**—Blackhole MAC address entry. • **Multiport**—Multiport unicast MAC address entry. • **OpenFlow**—MAC address entry for an OpenFlow instance. • **Block**—MAC address entry for a user who failed MAC authentication.
Port/Nickname	When the field displays an interface name, the field indicates the outgoing interface for packets that are destined for the MAC address. This field displays **N/A** for a blackhole MAC address entry.
Aging	Whether the entry can age out: • **Y**—The entry can age out. • **N**—The entry never ages out.
mac address(es) found	Number of matching MAC address entries.

Related commands

mac-address

mac-address timer

display mac-address aging-time

Use **display mac-address aging-time** to display the aging timer for dynamic MAC address entries.

Syntax

display mac-address aging-time

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the aging timer for dynamic MAC address entries.

```
<Sysname> display mac-address aging-time
MAC address aging time: 300s.
```

Related commands

mac-address timer

display mac-address hash-bucket-size

Use **display mac-address hash-bucket-size** to display the hash bucket size for the MAC address table.

Syntax

display mac-address hash-bucket-size

Views

Any view

Predefined user roles

network-admin

Usage guidelines

Examples

Display the hash bucket size for the MAC address table.

```
<Sysname> display mac-address hash-bucket-size
  Hash-bucket-size in use: 4
  Hash-bucket-size at the next reboot: 8
```

Table 2 Command output

Field	Description
Hash-bucket-size in use	Current hash bucket size.
Hash-bucket-size at the next reboot	Hash bucket size that will take effect at the next startup.

Related commands

mac-address hash-bucket-size

display mac-address hash-conflict-record

Use **display mac-address hash-conflict-record** to display the log messages generated for MAC hashing conflicts.

NOTE:

This command is supported only in Release 6328 and later.

Syntax

display mac-address hash-conflict-record slot *slot-number*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID.

Usage guidelines

A device enabled with MAC hashing conflict logging records the MAC hashing conflicts that occur in MAC address learning. To identify the MAC addresses that the device fails to learn, you can execute this command to display the log messages generated for MAC hashing conflicts. The output fields of this command are displayed only when the MAC hashing conflict logging feature is enabled.

Examples

Display the log messages generated for MAC hashing conflicts on slot 1.

```
<Sysname> display mac-address hash-conflict-record slot 1
MAC Address      VLAN     Port                      Count  Timestamp
0001-0101-0101   100      GE1/0/1                   1      2020/11/11 21:11:29
0000-0000-0002   100      GE1/0/3                   1      2020/11/11 21:11:29
00e0-fc00-5829   100      GE1/0/4                   1      2020/11/11 21:11:29
```

Table 3 Command output

Field	Description
MAC Address	MAC address that the device fails to learn because of MAC hashing conflicts.
VLAN	VLAN to which the outgoing interface of the MAC address entry belongs.
Port	Outgoing interface of the MAC address entry.
Count	Number of MAC hashing conflicts for the MAC address and VLAN after the MAC hashing conflict logging feature is enabled.
Timestamp	Last time when the MAC hashing conflict occurs.

Related commands

mac-address hash-conflict-record enable

display mac-address mac-learning

Use **display mac-address mac-learning** to display the global MAC address learning status and the MAC learning status of the specified interface or all interfaces.

Syntax

display mac-address mac-learning [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, the command displays the global MAC address learning status and the MAC address learning status of all interfaces.

Examples

Display the global MAC address learning status and the MAC learning status of all interfaces.

```
<Sysname> display mac-address mac-learning
Global MAC address learning status: Enabled.

Port                        Learning Status
GE1/0/1                     Enabled
GE1/0/2                     Enabled
```

Table 4 Command output

Field	Description
Global MAC address learning status	Global MAC address learning status: • Enabled. • Disabled.
Learning Status	MAC address learning status of an interface: • Enabled. • Disabled.

Related commands

mac-address mac-learning enable

display mac-address mac-move

Use **display mac-address mac-move** to display the MAC address move records after the device is started.

Syntax

display mac-address mac-move [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, the command displays MAC address move records for all IRF member devices.

Usage guidelines

When a MAC address frequently moves between the specified two interfaces, Layer 2 loops might occur in the network. To discover and locate loops, you can view the MAC address move records.

In the MAC address move records, records with the same MAC address, VLAN, source port, and current port are considered to be one record.

An IRF member device can generate a maximum of 200 MAC address move records.

Examples

Display the MAC address move records for a slot.

```
<Sysname> display mac-address mac-move slot 1
MAC address    VLAN Current port  Source port   Last time           Times
0000-0001-002c 1    GE1/0/1       GE1/0/2       2013-05-20 13:40:52 1
0000-0001-002c 1    GE1/0/2       GE1/0/1       2013-05-20 13:41:30 1
---  2 MAC address moving records found  ---
```

Display the MAC address move records for all slots.

```
<Sysname> display mac-address mac-move
MAC address    VLAN Current port  Source port   Last time           Times
0000-0001-002c 1    GE1/0/1       GE1/0/2       2013-05-20 13:40:52 20
0000-0001-002c 1    GE1/0/2       GE1/0/1       2013-05-20 13:41:32 20
0000-0094-0001 1    GE1/0/3       GE1/0/4       2013-05-20 13:42:22 13
0000-0094-0001 1    GE1/0/4       GE1/0/3       2013-05-20 13:42:21 12
---  4 MAC address moving records found  ---
```

Table 5 Command output

Field	Description
VLAN	VLAN to which the outgoing interface of the MAC address entry belongs.
Current port	Interface to which the MAC address was moved.
Source port	Interface from which the MAC address was moved.
Last time	Last time when the MAC address was moved.
Times	Number of MAC address moves after the device is started. For a MAC address record, the number of MAC address moves is increased by 1 when a new MAC address move has the same **MAC address**, **VLAN**, **Current Port**, and **Source Port** fields as the MAC address record.

Related commands

mac-address notification mac-move

display mac-address statistics

Use **display mac-address statistics** to display MAC address table statistics.

Syntax

display mac-address statistics

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

This command displays the number of MAC address entries per type and the maximum number of MAC address entries allowed for each type.

Examples

Display MAC address table statistics.

```
<Sysname> display mac-address statistics
MAC Address Count:
Dynamic Unicast Address (Learned) Count:                        3
Dynamic Unicast Address (Security-service-defined) Count:       4
Static Unicast Address (User-defined) Count:                    0
Static Unicast Address (System-defined) Count:                  3
Total Unicast MAC Addresses In Use:                             10
Total Unicast MAC Addresses Available:                          16384
Multicast and Multiport MAC Address Count:                      1
Static Multicast and Multiport MAC Address (User-defined) Count: 1
Total Multicast and Multiport MAC Addresses Available:          256
```

Table 6 Command output

Field	Description
Dynamic Unicast Address (Learned) Count	Number of dynamic unicast MAC address entries triggered by packets.
Dynamic Unicast Address (Security-service-defined) Count	Number of dynamic unicast MAC address entries triggered by the security service.
Static Unicast Address (User-defined) Count	Number of static unicast MAC address entries added by users.
Static Unicast Address (System-defined) Count	Number of static unicast MAC address entries added by the system.
Total Unicast MAC Addresses In Use	Number of unicast MAC address entries.
Total Unicast MAC Addresses Available	Maximum number of unicast MAC address entries allowed.
Multicast and Multiport MAC Address Count	Number of multicast and multiport unicast MAC address entries.
Static Multicast and Multiport MAC Address (User-defined) Count	Number of static multicast and multiport unicast MAC address entries added by users.
Total Multicast and Multiport MAC Addresses Available	Maximum number of multicast and multiport unicast MAC address entries allowed.

mac-address (interface view)

Use **mac-address** to add or modify a MAC address entry on an interface.

Use **undo mac-address** to delete a MAC address entry on an interface.

Syntax

mac-address { **dynamic** | **multiport** | **static** } *mac-address* **vlan** *vlan-id*

undo mac-address { **dynamic** | **multiport** | **static** } *mac-address* **vlan** *vlan-id*

Default

An interface is not configured with MAC address entries.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

dynamic: Specifies dynamic MAC address entries.

static: Specifies static MAC address entries.

multiport: Specifies multiport unicast MAC address entries. A frame whose destination MAC address matches a multiport unicast MAC address entry is sent out of multiple ports.

mac-address: Specifies a MAC address in the format of H-H-H, excluding multicast, all-zero, and all-F MAC addresses. When entering a MAC address, you can omit the leading zeros in each H section. For example, enter f-e2-1 for 000f-00e2-0001.

vlan *vlan-id*: Specifies an existing VLAN to which the specified interface belongs. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

Typically, the device automatically builds the MAC address table by learning the source MAC addresses of incoming frames on each interface. However, you can manually configure static MAC address entries. For a MAC address, a manually configured static entry takes precedence over a dynamically learned entry. To improve the security for the user device connected to an interface, manually configure a static entry to bind the user device to the interface. Then, the frames destined for the user device (for example, Host A) are always sent out of the interface. Other hosts using the forged MAC address of Host A cannot obtain the frames destined for Host A.

The MAC address entry configuration cannot survive a reboot unless you save it. The dynamic MAC address entries, however, are lost upon reboot whether or not you save the configuration.

Examples

Add a static entry for MAC address 000f-e201-0101 on GigabitEthernet 1/0/1 that belongs to VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-address static 000f-e201-0101 vlan 2
```

Add a static entry for MAC address 000f-e201-0101 on Bridge-Aggregation 1 that belongs to VLAN 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] mac-address static 000f-e201-0102 vlan 1
```

Add a multiport unicast MAC address entry for MAC address 0001-0001-0101 on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 that belong to VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-address multiport 0001-0001-0101 vlan 2
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] mac-address multiport 0001-0001-0101 vlan 2
```

Related commands

display mac-address

mac-address (system view)

mac-address (system view)

Use **mac-address** to add or modify a MAC address entry.

Use **undo mac-address** to delete one or all MAC address entries.

Syntax

mac-address { **dynamic** | **static** } *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*

mac-address blackhole *mac-address* **vlan** *vlan-id*

mac-address multiport *mac-address* **interface** *interface-list* **vlan** *vlan-id*

undo mac-address [[**dynamic** | **static**] *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*]

undo mac-address [**blackhole** | **dynamic** | **static**] [*mac-address*] **vlan** *vlan-id*

undo mac-address [**dynamic** | **static**] **interface** *interface-type interface-number*

undo mac-address multiport *mac-address* **interface** *interface-list* **vlan** *vlan-id*

undo mac-address [**multiport**] [[*mac-address*] **vlan** *vlan-id*]

Default

The system is not configured with MAC address entries.

Views

System view

Predefined user roles

network-admin

Parameters

dynamic: Specifies dynamic MAC address entries.

static: Specifies static MAC address entries.

blackhole: Specifies blackhole MAC address entries. Packets whose source or destination MAC addresses match blackhole MAC address entries are dropped.

multiport: Specifies multiport unicast MAC address entries. A frame whose destination MAC address matches a multiport unicast MAC address entry is sent out of multiple ports.

mac-address: Specifies a MAC address in the format of H-H-H, excluding multicast, all-zero, and all-F MAC addresses. When entering a MAC address, you can omit the leading zeros in each H section. For example, enter f-e2-1 for 000f-00e2-0001.

vlan *vlan-id*: Specifies an existing VLAN to which the interface belongs. The value range for the *vlan-id* argument is 1 to 4094.

interface *interface-type interface-number*: Specifies an outgoing interface by its type and number.

interface *interface-list*: Specifies a list of up to four interface items. Each interface item can be an individual interface in the format of *interface-type interface-number* or a range of interfaces in the format of *interface-type interface-number1* **to** *interface-type interface-number2*. The interfaces can only be Layer 2 Ethernet interfaces or Layer 2 aggregate interfaces. The value for the *interface-number2* argument cannot be lower than the value for the *interface-number1* argument.

Usage guidelines

You can use this command to configure the following types of MAC address entries:

- Dynamic entries.

  Dynamic entries include manually configured dynamic entries and automatically learned dynamic entries.

- Static entries.

  For a MAC address, a manually configured static entry takes precedence over a dynamic entry. To improve the security for the user device connected to an interface, manually configure a static entry to bind the user device to the interface. Then, the frames destined for the user device (for example, Host A) are always sent out of the interface. Other hosts using the forged MAC address of Host A cannot obtain the frames destined for Host A.

- Blackhole entries.

  To drop frames with the specified source MAC addresses or destination MAC addresses, you can configure blackhole entries.

- Multiport unicast entries.

  To send frames with a specific destination MAC address out of multiple ports, configure a multiport unicast entry. When you execute this command for the first time, the command adds an entry. When you execute the command again with the same MAC address and VLAN but with different interfaces, this command adds the specified interfaces for this entry.

A static or blackhole entry can overwrite a dynamic entry, but not vice versa.

If you execute the **undo mac-address** command without specifying any parameters, this command deletes all unicast MAC address entries and static multicast MAC address entries.

You can delete all the MAC address entries (including unicast and static multicast MAC address entries) from the specified VLAN. You can also delete only one type (dynamic, static, blackhole, or multiport unicast) of MAC address entries. You can single out an interface and delete the unicast MAC address entries on it, but not the static multicast MAC address entries.

The MAC address entry configuration cannot survive a reboot unless you save it. The dynamic MAC address entries, however, are lost upon reboot whether or not you save the configuration.

Examples

Add a static entry for MAC address 000f-e201-0101. Then, all frames that are destined for this MAC address are sent out of GigabitEthernet 1/0/1, which belongs to VLAN 2.

```
<Sysname> system-view
[Sysname] mac-address static 000f-e201-0101 interface gigabitethernet 1/0/1 vlan 2
```

Add a multiport unicast MAC address entry for MAC address 000f-e201-0101. Then, all frames that are destined for this MAC address are sent out of GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3, which belong to VLAN 2.

```
<Sysname> system-view
[Sysname] mac-address multiport 000f-e201-0101 interface gigabitethernet 1/0/1 to
gigabitethernet 1/0/3 vlan 2
```

Related commands

display mac-address

mac-address (interface view)

mac-address hash-bucket-size

Use **mac-address hash-bucket-size** to set the hash bucket size of the MAC address table.

Use **undo mac-address hash-bucket-size** to restore the default.

Syntax

mac-address hash-bucket-size *size*

undo mac-address hash-bucket-size

Default

The hash bucket size of the MAC address table is 4.

Views

System view

Predefined user roles

network-admin

Parameters

size: Sets the hash bucket size. Available values are 4, 8, and 16.

Usage guidelines

The device saves the MAC address table through hash chains. If multiple MAC addresses obtain the same key through hashing, MAC address hash conflicts occur, and the device cannot learn some of these MAC addresses. The device will broadcast the traffic destined for the unknown MAC addresses, which consumes bandwidth and resources.

You can increase the hash bucket size of the MAC address table to reduce MAC address hash conflicts. A larger hash bucket size requires more system resources. Please set the hash bucket size appropriately depending on system resources.

The set hash bucket size takes effect at the next startup.

Examples

Set the hash bucket size of the MAC address table to 8.

```
<Sysname> system-view
[Sysname] mac-address hash-bucket-size 8
The configuration will take effect at the next reboot. Continue? [Y/N]:y
Reboot device to make the configuration take effect.
```

Related commands

display mac-address hash-bucket-size

mac-address hash-conflict-record enable

Use **mac-address hash-conflict-record enable** to enable MAC hashing conflict logging.

Use **undo mac-address hash-conflict-record enable** to disable MAC hashing conflict logging.

NOTE:

This command is supported only in Release 6328 and later.

Syntax

mac-address hash-conflict-record enable slot *slot-number*

undo mac-address hash-conflict-record enable slot *slot-number*

Default

MAC hashing conflict logging is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID.

Usage guidelines

The device generates a unique hashing key for each MAC address when learning MAC addresses. If the device incorrectly generates the same hashing key for multiple MAC addresses, it might fail to learn some of the MAC addresses. MAC hashing conflict logging enables the device to record the MAC hashing conflicts that occur in MAC address learning. You can use this feature to identify the MAC addresses that the device fails to learn because of hashing conflicts. To display the log messages generated for MAC hashing conflicts, execute the **display mac-address hash-conflict-record** command.

This feature consumes system resources. When you enable it on the device, make sure you are fully aware of the impact on device performance.

Examples

Enable MAC hashing conflict logging on slot 1.

```
<Sysname> system-view
[Sysname] mac-address hash-conflict-record enable slot 1
```

Related commands

display mac-address hash-conflict-record

mac-address mac-learning enable

Use **mac-address mac-learning enable** to enable MAC address learning globally, on an interface, or on a VLAN.

Use **undo mac-address mac-learning enable** to disable MAC address learning globally, on an interface, or on a VLAN.

Syntax

mac-address mac-learning enable

undo mac-address mac-learning enable

Default

MAC address learning is enabled.

Views

System view

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

VLAN view

Predefined user roles

network-admin

Usage guidelines

To prevent the MAC address table from becoming saturated, you can disable MAC address learning.

For example, a number of packets with different source MAC addresses reaching a device can affect the MAC address table update. To avoid such attacks, you can disable MAC address learning by following these guidelines:

- You can disable MAC address learning on a per-interface basis. If you disable MAC address learning globally, MAC address learning is disabled for all interfaces. The device then stops learning MAC addresses and cannot dynamically update the MAC address table.
- Because disabling MAC address learning can result in broadcast storms, enable broadcast storm suppression after you disable MAC address learning on an interface. For more information about broadcast storm suppression, see *Interface Configuration Guide*.
- With MAC address learning enabled globally, you can disable MAC address learning for an interface or VLAN.
- After MAC address learning is disabled, the device immediately deletes existing dynamic MAC address entries.

Examples

Disable MAC address learning globally.

```
<Sysname> system-view
[Sysname] undo mac-address mac-learning enable
```

Disable MAC address learning for VLAN 10.

```
<Sysname> system-view
[Sysname] vlan 10
[Sysname-vlan10] undo mac-address mac-learning enable
```

Disable MAC address learning on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo mac-address mac-learning enable
```

Disable MAC address learning on Bridge-Aggregation 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] undo mac-address mac-learning enable
```

Related commands

display mac-address mac-learning

mac-address mac-move fast-update

Use **mac-address mac-move fast-update** to enable ARP fast update for MAC address moves.

Use **undo mac-address mac-move fast-update** to disable ARP fast update for MAC address moves.

Syntax

mac-address mac-move fast-update

undo mac-address mac-move fast-update

Default

ARP fast update is disabled for MAC address moves.

Views

System view

Predefined user roles

network-admin

Examples

Enable ARP fast update for MAC address moves.

```
<Sysname> system-view
[Sysname] mac-address mac-move fast-update
```

mac-address mac-roaming enable

Use **mac-address mac-roaming enable** to enable MAC address synchronization.

Use **undo mac-address mac-roaming enable** to disable MAC address synchronization.

Syntax

mac-address mac-roaming enable

undo mac-address mac-roaming enable

Default

MAC address synchronization is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

On an IRF fabric, if ports on different IRF member devices are Selected ports from the same aggregation group, MAC address entries are synchronized among these IRF member devices. They are synchronized whether or not MAC address synchronization is enabled for the IRF fabric. For more information about aggregation groups, see *Layer 2—LAN Switching Configuration Guide*.

The MAC address table size might vary by IRF member device. With MAC address synchronization enabled, MAC address entries exceeding the table size of an IRF member device cannot be synchronized to the MAC address table.

Examples

Enable MAC address synchronization.

```
<Sysname> system-view
[Sysname] mac-address mac-roaming enable
```

mac-address max-mac-count

Use **mac-address max-mac-count** to set the MAC learning limit on an interface.

Use **undo mac-address max-mac-count** to restore the default.

Syntax

mac-address max-mac-count *count*

undo mac-address max-mac-count

Default

The number of MAC addresses that can be learned on an interface is not limited.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

count: Specifies the maximum number of MAC addresses that can be learned on an interface. When the argument is set to 0, the interface is not allowed to learn MAC addresses. The value range for this argument is 0 to 4096.

Usage guidelines

This command helps limit the MAC address table size. When the number of MAC address entries learned by an interface reaches the limit, the interface stops learning MAC address entries.

Examples

Configure GigabitEthernet 1/0/1 to learn a maximum of 600 MAC address entries.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-address max-mac-count 600
```

Related commands

mac-address

mac-address max-mac-count enable-forwarding

mac-address max-mac-count enable-forwarding

Use **mac-address max-mac-count enable-forwarding** to enable the device to forward unknown frames received on an interface after the MAC learning limit on the interface is reached. Unknown frames refer to frames whose source MAC addresses are not in the MAC address table.

Use **undo mac-address max-mac-count enable-forwarding** to disable the device from forwarding unknown frames received on an interface after the MAC learning limit on the interface is reached.

Syntax

mac-address max-mac-count enable-forwarding

undo mac-address max-mac-count enable-forwarding

Default

When the MAC learning limit on an interface is reached, the device can forward unknown frames received on the interface.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Examples

Configure GigabitEthernet 1/0/1 to learn a maximum of 600 MAC address entries.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-address max-mac-count 600
```

Disable the device from forwarding unknown frames received on GigabitEthernet 1/0/1 after the MAC learning limit on GigabitEthernet 1/0/1 is reached.

```
[Sysname-GigabitEthernet1/0/1] undo mac-address max-mac-count enable-forwarding
```

Related commands

mac-address

mac-address max-mac-count

mac-address multicast-source packet-filter

Use **mac-address multicast-source packet-filter** to enable packet filter on the device where its source MAC address is a multicast or broadcast MAC address.

Use **undo mac-address multicast-source packet-filter** to disable packet filter on the device where its source MAC address is a multicast or broadcast MAC address.

Syntax

mac-address multicast-source packet-filter

undo mac-address multicast-source packet-filter

Default

Packet filter is enabled on the device where its source MAC address is a multicast or broadcast MAC address.

Views

System view

Predefined user roles

network-admin

Usage guidelines

By default, the device will drop a frame whose source MAC address is a multicast or broadcast MAC address. To avoid the user traffic loss and ensure user trasffic to be forwarded correctly in this scenario, you can disable packet filter on the device where its source MAC address is a multicast or broadcast MAC address.

Examples

Disable packet filter when the source MAC address is a multicast or broadcast MAC address.

```
<Sysname> system-view
[Sysname] undo mac-address multicast-source packet-filter
```

mac-address notification mac-move

Use **mac-address notification mac-move** to enable MAC address move notifications and optionally specify a MAC move detection interval.

Use **undo mac-address notification mac-move** to disable MAC address move notifications.

Syntax

mac-address notification mac-move [**interval** *interval*]

undo mac-address notification mac-move

Default

MAC address move notifications are disabled.

Views

System view

Predefined user roles

network-admin

Parameters

interval *interval*: Specifies the interval for detecting MAC address moves, in the range of 1 to 60 minutes. If you do not specify this option, the default setting of 1 minute is used.

Usage guidelines

With MAC address move notifications enabled, the system records the MAC address move logs every MAC move detection interval. Each record of the MAC address move logs contains the following information:

- MAC address.
- VLAN ID of the MAC address entry.
- Current port and source port of the MAC address moves.
- Number of MAC address moves within a detection interval.

A MAC address can have only one MAC address move record. If a MAC address moves multiple times, the new record overrides the old record.

Within a detection interval, an IRF member device can record MAC address move information for a maximum of 20 MAC addresses. The records are ranked in descending order of MAC move counts. If the number of MAC address move records exceeds 20, only the first 20 records are retained. Then in the next detection interval, the device discards all MAC address move records generated in the previous detection interval and starts another round of MAC move record generation.

After you execute this command, the system sends only syslog messages to the information center module. If the **snmp-agent trap enable mac-address** command is also executed, the system also sends SNMP notifications to the SNMP module.

Examples

Enable MAC address move notifications.

```
<Sysname> system-view
[Sysname] mac-address notification mac-move
[Sysname]
%May 14 17:16:45:688 2013 Sysname MAC/4/MAC_NOTIFICATION: MAC address 0000-0012-0034 in VLAN 500 has moved from port GE1/0/1 to port GE1/0/2 for 1 times
```

The output shows that:

- The VLAN ID of MAC address 0000-0012-0034 is VLAN 500.
- The MAC address moved from GigabitEthernet 1/0/1 to GigabitEthernet 1/0/2.
- The MAC address has moved once within a MAC move detection interval.

Related commands

display mac-address mac-move

mac-address notification mac-move suppression (interface view)

Use **mac-address notification mac-move suppression** to enable MAC address move suppression on an interface.

Use **undo mac-address notification mac-move suppression** to disable MAC address move suppression on an interface.

Syntax

mac-address notification mac-move suppression

undo mac-address notification mac-move suppression

Default

MAC address moves are not suppressed.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

This feature shuts an interface down when a MAC address has been moved to or from the interface more than the suppression threshold within a MAC move detection interval. The shutdown interface automatically goes up after a suppression interval. Also, you can use the **shutdown** command and then the **undo shutdown** command to bring up the interface.

When MAC address move suppression shuts an interface down, the system sends only syslog messages to the information center module. If the **snmp-agent trap enable mac-address** command is also executed, the system also sends SNMP notifications to the SNMP module.

Examples

Enable MAC address move suppression on GigabitEthernet 1/0/1.

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-address notification mac-move suppression
```

Related commands

mac-address notification mac-move suppression (system view)

mac-address notification mac-move suppression (system view)

Use **mac-address notification mac-move suppression** to set the suppression interval or the suppression threshold.

Use **undo mac-address notification mac-move suppression** to restore the default.

Syntax

mac-address notification mac-move suppression { **interval** *interval* | **threshold** *threshold* }

undo mac-address notification mac-move suppression { **interval** | **threshold** }

Default

The suppression interval is 30 seconds. The suppression threshold is 3.

Views

System view

Predefined user roles

network-admin

Parameters

interval *interval*: Specifies the MAC address move suppression interval during which a suppressed interface stays down. The value range for the *interval-value* argument is 30 to 86400 seconds. If you do not specify this option, the default suppression interval of 30 seconds is used.

threshold *threshold*: Specifies the suppression threshold for MAC address moves sourced from or destined for an interface within a MAC move detection interval. The value range for this argument is 0 to 1024. If you do not specify this option, the default suppression threshold of 3 is used.

Usage guidelines

For this command to take effect on an interface, you must also enable MAC address move suppression on the interface.

If you set the suppression interval or suppression threshold multiple times, the most recent configuration applies. The suppression interval setting is independent of the suppression threshold setting.

Examples

Set the suppression interval to 40 seconds and the suppression threshold to 1 for MAC address moves.

```
<Sysname> system-view
[Sysname] mac-address notification mac-move suppression interval 40
```

```
[Sysname] mac-address notification mac-move suppression threshold 1
```

Related commands

mac-address notification mac-move suppression (interface view)

mac-address timer

Use **mac-address timer** to set the aging timer for dynamic MAC address entries.

Use **undo mac-address timer** to restore the default.

Syntax

mac-address timer { **aging** *seconds* | **no-aging** }

undo mac-address timer

Default

The aging timer is 300 seconds for dynamic MAC address entries.

Views

System view

Predefined user roles

network-admin

Parameters

aging *seconds*: Specifies an aging timer for dynamic MAC address entries, in seconds. The value range for the *seconds* argument is 10 to 630 in versions earlier than Release 6328. The value range for the *seconds* argument is 10 to 100000 in Release 6328 and later.

no-aging: Configures dynamic MAC address entries not to age.

Usage guidelines

To set the aging timer appropriately, follow these guidelines:

- A long aging interval causes the MAC address table to retain outdated entries and fail to accommodate the most recent network changes.
- A short aging interval results in removal of valid entries. Then, unnecessary broadcast packets appear and affect device performance.

Examples

Set the aging time to 500 seconds for dynamic MAC address entries.

```
<Sysname> system-view
[Sysname] mac-address timer aging 500
```

Related commands

display mac-address aging-time

snmp-agent trap enable mac-address

Use **snmp-agent trap enable mac-address** to enable SNMP notifications for the MAC address table.

Use **undo snmp-agent trap enable mac-address** to disable SNMP notifications for the MAC address table.

Syntax

snmp-agent trap enable mac-address [**mac-move**]

undo snmp-agent trap enable mac-address [**mac-move**]

Default

SNMP notifications are enabled for the MAC address table.

Views

System view

Predefined user roles

network-admin

Parameters

mac-move: Specifies notifications about the MAC address moves for the MAC address table. If you do not specify this keyword, the command enables all types of SNMP notifications for the MAC address table.

Usage guidelines

To report critical MAC address move events to an NMS, enable SNMP notifications for the MAC address table. For MAC address move event notifications to be sent correctly, you must also configure SNMP on the device.

When SNMP notifications are disabled for the MAC address table, the device sends the generated logs to the information center. To display the logs, configure the log destination and output rule configuration in the information center.

For information about SNMP and information center configuration, see the network management and monitoring configuration guide for the device.

The MAC address table supports only SNMP notifications about MAC address moves. When you enable or disable SNMP notifications about MAC address moves, you enable or disable all types of SNMP notifications for the MAC address table.

Examples

Disable SNMP notifications about MAC address moves for the MAC address table.

```
<Sysname> system-view
[Sysname] undo snmp-agent trap enable mac-address mac-move
```

Related commands

mac-address notification mac-move

MAC Information commands

mac-address information enable (interface view)

Use **mac-address information enable** to enable MAC Information on an interface.

Use **undo mac-address information enable** to disable MAC Information on an interface.

Syntax

mac-address information enable { **added** | **deleted** }

undo mac-address information enable { **added** | **deleted** }

Default

MAC Information is disabled on an interface.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

added: Enables the device to record MAC change information when a new MAC address is learned on an interface.

deleted: Enables the device to record MAC change information when an existing MAC address is deleted.

Usage guidelines

Before you enable MAC Information on an interface, enable MAC Information globally.

Examples

Enable MAC Information on GigabitEthernet 1/0/1 to enable the interface to record MAC change information when learning a new MAC address.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-address information enable added
```

Related commands

mac-address information enable (system view)

mac-address information enable (system view)

Use **mac-address information enable** to enable MAC Information globally.

Use **undo mac-address information enable** to disable MAC Information globally.

Syntax

mac-address information enable

undo mac-address information enable

Default

MAC Information is disabled globally.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Before you enable MAC Information on an interface, enable MAC Information globally.

Examples

Enable MAC Information globally.

```
<Sysname> system-view
[Sysname] mac-address information enable
```

Related commands

mac-address information enable (interface view)

mac-address information interval

Use **mac-address information interval** to set the MAC change notification interval.

Use **undo mac-address information interval** to restore the default.

Syntax

mac-address information interval *interval*

undo mac-address information interval

Default

The MAC change notification interval is 1 second.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the MAC change notification interval in the range of 1 to 20000 seconds.

Usage guidelines

To prevent syslog messages or SNMP notifications from being sent too frequently, set the MAC change notification interval to a larger value.

Examples

Set the MAC change notification interval to 200 seconds.

```
<Sysname> system-view
[Sysname] mac-address information interval 200
```

mac-address information mode

Use **mac-address information mode** to set the MAC Information mode. The MAC Information mode specifies the type of messages (syslog messages or SNMP notifications) used to notify MAC changes.

Use **undo mac-address information mode** to restore the default.

Syntax

mac-address information mode { **syslog** | **trap** }

undo mac-address information mode

Default

SNMP notifications are sent to notify MAC changes.

Views

System view

Predefined user roles

network-admin

Parameters

syslog: Specifies that the device sends syslog messages to notify MAC changes.

trap: Specifies that the device sends SNMP notifications to notify MAC changes.

Examples

Configure the MAC Information mode as **trap**.

```
<Sysname> system-view
[Sysname] mac-address information mode trap
```

mac-address information queue-length

Use **mac-address information queue-length** to set the MAC Information queue length.

Use **undo mac-address information queue-length** to restore the default.

Syntax

mac-address information queue-length *value*

undo mac-address information queue-length

Default

The MAC Information queue length is 50.

Views

System view

Predefined user roles

network-admin

Parameters

value: Specifies the MAC Information queue length in the range of 0 to 1000. The MAC Information queue length indicates the number of MAC change messages.

Usage guidelines

If the MAC Information queue length is 0, the device sends a syslog message or SNMP notification immediately after learning or deleting a MAC address.

If the MAC Information queue length is not 0, the device stores MAC changes in the queue:

- The device overwrites the oldest MAC change written into the queue with the most recent MAC change when the following conditions exist:
  - The MAC change notification interval does not expire.
  - The queue has been exhausted.

- The device sends syslog messages or SNMP notifications only if the MAC change notification interval expires.

Examples

Set the MAC Information queue length to 600.

```
<Sysname> system-view
[Sysname] mac-address information queue-length 600
```

Contents

Ethernet link aggregation commands

bandwidth

Use **bandwidth** to set the expected bandwidth for an interface.

Use **undo bandwidth** to restore the default.

Syntax

bandwidth *bandwidth-value*

undo bandwidth

Default

The expected bandwidth (in kbps) is the interface baud rate divided by 1000.

Views

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

bandwidth-value: Specifies the expected bandwidth in the range of 1 to 400000000 kbps.

Usage guidelines

The expected bandwidth is an informational parameter used only by higher-layer protocols for calculation. You cannot adjust the actual bandwidth of an interface by using this command.

Examples

Set the expected bandwidth to 10000 kbps for Layer 2 aggregate interface Bridge-Aggregation 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] bandwidth 10000
```

default

Use **default** to restore the default settings for an aggregate interface.

Syntax

default

Views

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

△ **CAUTION:**

The **default** command might interrupt ongoing network services. Make sure you are fully aware of the impacts of this command when you execute it on a live network.

This command might fail to restore the default settings for some commands for reasons such as command dependencies and system restrictions. Use the **display this** command in interface view to identify these commands, and then use their **undo** forms or follow the command reference to restore their default settings. If your restoration attempt still fails, follow the error message instructions to resolve the problem.

Examples

Restore the default settings for Layer 2 aggregate interface 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] default
```

description

Use **description** to configure the description of an interface.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

The description of an interface is *interface-name* **Interface**. For example, the default description of Bridge-Aggregation 1 is **Bridge-Aggregation1 Interface**.

Views

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 255 characters.

Examples

Configure the description as **connect to the lab** for Layer 2 aggregate interface Bridge-Aggregation 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] description connect to the lab
```

display interface

Use **display interface** to display aggregate interface information.

Syntax

display interface [**bridge-aggregation** [*interface-number*]] [**brief** [**description** | **down**]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

bridge-aggregation: Specifies Layer 2 aggregate interfaces.

interface-number: Specifies an existing aggregate interface number.

brief: Displays brief interface information. If you do not specify this keyword, the command displays detailed interface information.

description: Displays complete interface descriptions. If you do not specify this keyword, the command displays only the first 27 characters of each interface description.

down: Displays information about interfaces in down state and the causes for the down state. If you do not specify this keyword, the command displays information about interfaces in all states.

Usage guidelines

If you do not specify an aggregate interface type, the command displays information about all interfaces.

If you specify an aggregate interface type but do not specify an interface number, the command displays information about all aggregate interfaces of the specified type.

Examples

Display detailed information about Layer 2 aggregate interface Bridge-Aggregation 1.

```
<Sysname> display interface bridge-aggregation 1
Bridge-Aggregation1
Current state: UP
Line protocol state: UP
IP packet frame type: Ethernet II, hardware address: 000f-e207-f2e0
Description: Bridge-Aggregation1 Interface
Bandwidth: 1000 kbps
2Gbps-speed mode, full-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
PVID: 1
Port link-type: Access
 Tagged VLANs:   None
 UnTagged VLANs: 1
Last clearing of counters: Never
Last 300 seconds input:  6900 packets/sec 885160 bytes/sec    0%
Last 300 seconds output:  3150 packets/sec 404430 bytes/sec    0%
Input (total):  5364747 packets, 686688416 bytes
         2682273 unicasts, 1341137 broadcasts, 1341337 multicasts, 0 pauses
Input (normal):  5364747 packets, 686688416 bytes
         2682273 unicasts, 1341137 broadcasts, 1341337 multicasts, 0 pauses
Input:  0 input errors, 0 runts, 0 giants, 0 throttles
         0 CRC, 0 frame, 0 overruns, - aborts
         - ignored, - parity errors
Output (total): 1042508 packets, 133441832 bytes
         1042306 unicasts, 0 broadcasts, 202 multicasts, - pauses
Output (normal): 1042508 packets, 133441832 bytes
         1042306 unicasts, 0 broadcasts, 202 multicasts, 0 pauses
```

```
Output: 0 output errors, - underruns, - buffer failures
         0 aborts, 0 deferred, 0 collisions, 0 late collisions
         - lost carrier, - no carrier
```

Display brief information about Layer 2 aggregate interface Bridge-Aggregation 1.

```
<Sysname> display interface bridge-aggregation 1 brief
Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) – auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface            Link Speed   Duplex Type PVID Description
BAGG1                DOWN auto    A      A    1
```

Table 1 Command output

Field	Description
Bridge-Aggregation1	Layer 2 aggregate interface name.
Current state	Physical link state of the interface: • **Administratively DOWN**—The interface has been shut down by using the **shutdown** command. • **DOWN**—The interface is administratively up, but its physical state is down (possibly because no physical link exists or the link has failed). • **UP**—The interface is both administratively and physically up.
IP packet frame type	IPv4 packet framing format.
Description	Description of the interface.
Bandwidth	Expected bandwidth of the interface. This field is not displayed when the bandwidth is 0 kbps.
Port priority	Port priority of the interface.
Unknown-speed mode, unknown-duplex mode	The interface speed and duplex mode are unknown.
Port link-type	Port link type: • Access. • Trunk. • Hybrid.
Tagged VLANs	VLAN whose packets are sent out of this interface with a tag.
Untagged VLANs	VLAN whose packets are sent out of this interface without a tag.
Last clearing of counters	Time when the **reset counters interface** command was last used to clear the interface statistics. This field displays **Never** if the **reset counters interface** command has never been used on the interface since device startup.
Last 300 seconds input/output rate	Average input or output rate over the last 300 seconds.
Input/Output (total)	Statistics of all packets received or sent on the interface.
Input/Output (normal)	Statistics of all normal packets received or sent on the interface.
Line protocol state	Data link layer state of the interface: • **UP**. • **DOWN**.

Field	Description
Maximum transmission unit	MTU of the interface.
Brief information on interfaces in bridge mode	Brief information about Layer 2 interfaces.
Interface	Abbreviated interface name.
Link	Physical link state of the interface: • **UP**—The interface is physically up. • **DOWN**—The interface is physically down. • **ADM**—The interface has been shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command.
Speed	Speed of the interface, in bps. This field displays the **(a)** flag next to the speed if the speed is automatically negotiated. This field displays **auto** if the interface is configured to autonegotiate its speed but the autonegotiation has not started.
Duplex	Duplex mode of the interface: • **A**—Autonegotiation. The interface is configured to autonegotiate its duplex mode but the autonegotiation has not started. • **F**—Full duplex. • **F(a)**—Autonegotiated full duplex. • **H**—Half duplex. • **H(a)**—Autonegotiated half duplex.
Type	Link type of the interface: • **A**—Access. • **H**—Hybrid. • **T**—Trunk.
Protocol	Data link layer protocol state of the interface: • **UP**—The data link layer protocol of the interface is up. • **DOWN**—The data link layer protocol of the interface is down. • **UP(s)**—The data link layer protocol of the interface is up, but the link is an on-demand link or does not exist. The **(s)** attribute represents the spoofing flag. This value is typical of null interfaces and loopback interfaces.
Cause	Cause for the physical link state of an interface to be **DOWN**.

display lacp system-id

Use **`display lacp system-id`** to display the local system ID.

Syntax

`display lacp system-id`

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

You can use the **lacp system-priority** command to change the LACP priority of the local system. The LACP priority value is specified in decimal format in the **lacp system-priority** command. However, it is displayed in hexadecimal format in the output from the **display lacp system-id** command.

Examples

Display the local system ID.

```
<Sysname> display lacp system-id
Actor System ID: 0x8000, 0000-fc00-6504
```

Table 2 Command output

Field	Description
Actor System ID: 0x8000, 0000-fc00-6504	Local system ID, which contains the LACP system priority (0x8000 in this sample output) and the LACP system MAC address (0000-FC00-6504 in this sample output).

Related commands

lacp system-priority

display link-aggregation load-sharing mode

Use **display link-aggregation load-sharing mode** to display global or group-specific link-aggregation load sharing modes.

Syntax

display link-aggregation load-sharing mode [**interface** [**bridge-aggregation** *interface-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

bridge-aggregation: Specifies Layer 2 aggregate interfaces.

interface-number: Specifies an existing aggregate interface number.

Usage guidelines

If you do not specify the **interface** keyword, the command displays the global link-aggregation load sharing modes.

If you specify the **interface** keyword, but do not specify an interface, the command displays all group-specific load sharing modes.

The **bridge-aggregation** keyword is available only when Layer 2 aggregate interfaces exist on the device.

Examples

Display the global link-aggregation load sharing mode. This example displays the default setting.

```
<Sysname> display link-aggregation load-sharing mode
Link-aggregation load-sharing mode:
Layer 2 traffic: packet type-based sharing
Layer 3 traffic: packet type-based sharing
```

Display the global link-aggregation load sharing mode. This example displays a user-configured setting.

```
<Sysname> display link-aggregation load-sharing mode
Link-aggregation load-sharing mode:
destination-mac address, source-mac address
```

Display the link-aggregation load sharing mode of Layer 2 aggregation group 10. This example displays the default setting.

```
<Sysname> display link-aggregation load-sharing mode interface bridge-aggregation 10
Bridge-Aggregation10 load-sharing mode:
Layer 2 traffic: packet type-based sharing
Layer 3 traffic: packet type-based sharing
```

Display the link-aggregation load sharing mode of Layer 2 aggregation group 10. This example displays a user-configured setting.

```
<Sysname> display link-aggregation load-sharing mode interface bridge-aggregation 10
Bridge-Aggregation10 load-sharing mode:
destination-mac address, source-mac address
```

Table 3 Command output

Field	Description
Link-aggregation load-sharing mode	Global link-aggregation load sharing mode. By default, this field displays the link-aggregation load sharing modes for Layer 2 and Layer 3 traffic. If you have configured the global link-aggregation load sharing mode, this field displays the configured mode.
Bridge-Aggregation10 load-sharing mode	Link-aggregation load sharing mode of Layer 2 aggregation group 10. By default, this field displays the global link-aggregation load sharing modes. If you have configured a link-aggregation load sharing mode for this aggregation group, this field displays the configured mode.
Layer 2 traffic: packet type-based sharing	Default link-aggregation load sharing mode for Layer 2 traffic. In this sample output, Layer 2 traffic is distributed based on the source and destination IP addresses and source and destination MAC addresses.
Layer 3 traffic: packet type-based sharing	Default link-aggregation load sharing mode for Layer 3 traffic. In this sample output, Layer 3 traffic is distributed based on the source and destination IP addresses and source and destination MAC addresses.
destination-mac address, source-mac address	User-configured link-aggregation load sharing mode. In this sample output, traffic is load shared based on source and destination MAC addresses.

display link-aggregation member-port

Use **display link-aggregation member-port** to display detailed link aggregation information about the specified member ports.

Syntax

display link-aggregation member-port [*interface-list* | **auto**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-list: Specifies a list of link aggregation member ports, in the format *interface-type interface-number1* [**to** *interface-type interface-number2*]. The value for the *interface-number2* argument must be equal to or greater than the value for the *interface-number1* argument.

auto: Specifies all link aggregation member ports that are enabled with automatic assignment.

Usage guidelines

A member port in a static aggregation group cannot obtain information about the peer group. For such member ports, the command displays the port number, port priority, and operational key of only the local end.

Examples

Display detailed information about GigabitEthernet 1/0/1, which is a member port of a static aggregation group.

```
<Sysname> display link-aggregation member-port gigabitethernet 1/0/1
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired

GigabitEthernet1/0/1:
Aggregate Interface: Bridge-Aggregation1
Port Number: 1
Port Priority: 32768
Oper-Key: 1
```

Display detailed information about GigabitEthernet 1/0/2, which is a member port of a dynamic aggregation group.

```
<Sysname> display link-aggregation member-port gigabitethernet 1/0/2
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired

GigabitEthernet1/0/2:
Aggregate Interface: Bridge-Aggregation10
Local:
    Port Number: 2
```

```
    Port Priority: 32768
    Oper-Key: 2
    Flag: {ACDEF}
Remote:
    System ID: 0x8000, 000f-e267-6c6a
    Port Number: 26
    Port Priority: 32768
    Oper-Key: 2
    Flag: {ACDEF}
Received LACP Packets: 5 packet(s)
Illegal: 0 packet(s)
Sent LACP Packets: 7 packet(s)
```

Display detailed information about all link aggregation member ports that are enabled with automatic assignment.

```
<Sysname> display link-aggregation member-port auto
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired

GigabitEthernet1/0/3:
Preference Aggregation Interface: Bridge-Aggregation11
Aggregate Interface: Bridge-Aggregation11
Local:
    Port Number: 3
    Port Priority: 32768
    Oper-Key: 1
    Flag: {ACDEF}
Remote:
    System ID: 0x8000, a057-75a2-0100
    Port Number: 3
    Port Priority: 32768
    Oper-Key: 1
    Flag: {ACDEF}
Received LACP Packets: 3 packet(s)
Illegal: 0 packet(s)
Sent LACP Packets: 6 packet(s)
```

Table 4 Command output

Field	Description
Flags	LACP state flags. This field is one byte long, represented by ABCDEFGH from the least significant bit to the most significant bit. A letter appears when its bit is 1 and does not appear when its bit is 0. • **A**—Indicates whether LACP is active on the port. 1 indicates active. 0 indicates passive. • **B**—Indicates the LACP timeout interval. 1 indicates the short timeout interval. 0 indicates the long timeout interval. • **C**—Indicates whether the sending system considers that the link is aggregatable. 1 indicates yes. 0 indicates no. • **D**—Indicates whether the sending system considers that the link has been aggregated. 1 indicates yes. 0 indicates no.

Field	Description
	• **E**—Indicates whether the sending system considers that the link can collect frames. 1 indicates yes. 0 indicates no. • **F**—Indicates whether the sending system considers that the link can distribute frames. 1 indicates yes. 0 indicates no. • **G**—Indicates whether the RX state machine of the sending system is in default state. 1 indicates yes. 0 indicates no. • **H**—Indicates whether the RX state machine of the sending system is in expired state. 1 indicates yes. 0 indicates no.
Aggregate Interface	Aggregate interface to which the member port belongs.
Preferred Aggregate Interface	Aggregate interface to which you prefer to assign the member port during automatic assignment.
Local	Information about the local end.
Oper-key	Operational key.
Flag	LACP protocol state flag.
Remote	Information about the peer end.
System ID	Peer system ID, containing the LACP system priority and the LACP system MAC address.
Received LACP Packets	Total number of LACP packets received.
Illegal	Total number of illegal packets.
Sent LACP Packets	Total number of LACP packets sent.

display link-aggregation summary

Use **display link-aggregation summary** to display brief information about all aggregation groups.

Syntax

display link-aggregation summary

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

Static link aggregation groups cannot obtain information about the peer groups. As a result, the **Partner ID** field displays **None** for a static link aggregation group.

Examples

Display brief information about all aggregation groups.

```
<Sysname> display link-aggregation summary
Aggregate Interface Type:
BAGG -- Bridge-Aggregation, BLAGG –- Blade-Aggregation, RAGG -- Route-Aggregation, SCH-B
– Schannel-Bundle
Aggregation Mode: S -- Static, D -- Dynamic
```

```
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Actor System ID: 0x8000, 000f-e267-6c6a

AGG        AGG   Partner ID              Selected  Unselected  Individual  Share
Interface  Mode                          Ports     Ports       Ports       Type
--------------------------------------------------------------------------------
BAGG20     D     0x8000,00e0-fcff-ff01   2         0           0           Shar
```

Table 5 Command output

Field	Description
Aggregate Interface Type	Aggregate interface type: • **BAGG**—Layer 2. • **RAGG**—Layer 3.
Aggregation Mode	Aggregation group type: • **S**—Static. • **D**—Dynamic.
Loadsharing Type	Load sharing type: • **Shar**—Load-sharing. • **NonS**—Non-load-sharing.
Actor System ID	Local system ID, which contains the local LACP system priority and the local LACP system MAC address.
AGG Interface	Type and number of the aggregate interface.
AGG Mode	Aggregation group type.
Partner ID	System ID of the peer system, which contains the peer LACP system priority and the peer LACP system MAC address.
Selected Ports	Total number of Selected ports.
Unselected Ports	Total number of Unselected ports.
Individual Ports	Total number of Individual ports.
Share Type	Load sharing type.

display link-aggregation verbose

Use **display link-aggregation verbose** to display detailed information about the aggregation groups that correspond to the specified aggregate interfaces.

Syntax

display link-aggregation verbose [**bridge-aggregation** [*interface-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

bridge-aggregation: Specifies Layer 2 aggregate interfaces.

interface-number: Specifies an existing aggregate interface by its number.

Usage guidelines

If you do not specify an aggregate interface type, the command displays detailed information about all aggregation groups.

If you specify an aggregate interface type but do not specify an interface number, the command displays detailed information about all aggregation groups of the specified type.

The **bridge-aggregation** keyword is available only when Layer 2 aggregate interfaces exist on the device.

This command does not display the interfaces that are enabled with automatic assignment if they have not joined an aggregation group.

Examples

Display detailed information about Layer 2 aggregation group 10, which is a dynamic aggregation group.

```
<Sysname> display link-aggregation verbose bridge-aggregation 10
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation10
Creation Mode: Manual
Aggregation Mode: Dynamic
Loadsharing Type: Shar
Management VLANs: None
System ID: 0x8000, 000f-e267-6c6a
Local:
  Port                Status   Priority Index    Oper-Key               Flag
  GE1/0/1             S        32768    61       2                      {ACDEF}
  GE1/0/2             S        32768    62       2                      {ACDEF}
  GE1/0/3             S        32768    63       2                      {AG}
Remote:
  Actor               Priority Index    Oper-Key SystemID               Flag
  GE1/0/1(R)          32768    111      2        0x8000, 000f-e267-57ad {ACDEF}
  GE1/0/2             32768    112      2        0x8000, 000f-e267-57ad {ACDEF}
  GE1/0/3             32768    113      0        0x8000, 0000-0000-0000 {DEF}
```

Display detailed information about Layer 2 aggregation group 20, which is a static aggregation group.

```
<Sysname> display link-aggregation verbose bridge-aggregation 20
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
```

```
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation20
Aggregation Mode: Static
Loadsharing Type: Shar
Management VLANs: None
  Port             Status  Priority Oper-Key
  GE1/0/1(R)       S       32768    1
  GE1/0/2          S       32768    1
  GE1/0/3          S       32768    1
```

Table 6 Command output

Field	Description
Loadsharing Type	Load sharing type: • **Shar**—Load-sharing. • **NonS**—Non-load-sharing.
Port Status	Port state: • **Selected**. • **Unselected**. • **Individual**.
Port	Port type: • **Auto port**—The port was assigned to the aggregation group by the automatic link aggregation feature or the automatic member port assignment feature. • **Management port**—The port is a management port. This value is not supported in the current software version. • **Reference port**—The port is a reference port.
Flags	LACP state flags. This field is one byte long, represented by ABCDEFGH from the least significant bit to the most significant bit. A letter appears when its bit is 1 and does not appear when its bit is 0. • **A**—Indicates whether LACP is active on the port. 1 indicates active. 0 indicates passive. • **B**—Indicates the LACP timeout interval. 1 indicates the short timeout interval. 0 indicates the long timeout interval. • **C**—Indicates whether the sending system considers that the link is aggregatable. 1 indicates yes. 0 indicates no. • **D**—Indicates whether the sending system considers that the link has been aggregated. 1 indicates yes. 0 indicates no. • **E**—Indicates whether the sending system considers that the link can collect frames. 1 indicates yes. 0 indicates no. • **F**—Indicates whether the sending system considers that the link can distribute frames. 1 indicates yes. 0 indicates no. • **G**—Indicates whether the RX state machine of the sending system is in default state. 1 indicates yes. 0 indicates no. • **H**—Indicates whether the RX state machine of the sending system is in expired state. 1 indicates yes. 0 indicates no.
Aggregate Interface	Name of the aggregate interface.
Creation Mode	Creation mode of the dynamic aggregate interface: • **Auto**. • **Manual**.
Aggregation Mode	Aggregation group type:

Field	Description
	• **S**—Static. • **D**—Dynamic.
Management VLANs	(This field is not supported in the current software version.) Management VLANs. If no management VLANs are specified, this field displays **None**.
System ID	Local system ID, containing the local LACP system priority and the local LACP system MAC address.
Local	Information about the local end: • **Port**—Port type and number. • **Status**—Port state, which can be Selected, Unselected, or Individual. • **Priority**—Port priority. • **Index**—Port index. • **Oper-Key**—Operational key. • **Flag**—LACP state flag. **NOTE:** For static aggregation groups, the **Index** and **Flag** fields are not displayed.
Remote	Information about the peer end: • **Actor**—Type and number of the local port. This field displays the **(R)** flag next to the port if its peer port is the reference port. • **Priority**—Priority of the peer port. • **Index**—Index of the peer port. • **Oper-Key**—Operational key of the peer port. • **System ID**—System ID of the peer end. • **Flag**—LACP state flag of the peer end.

interface bridge-aggregation

Use **`interface bridge-aggregation`** to create a Layer 2 aggregate interface and enter its view, or enter the view of an existing Layer 2 aggregate interface.

Use **`undo interface bridge-aggregation`** to delete a Layer 2 aggregate interface.

Syntax

`interface bridge-aggregation` *`interface-number`*

`undo interface bridge-aggregation` *`interface-number`*

Default

No Layer 2 aggregate interfaces exist.

Views

System view

Predefined user roles

network-admin

Parameters

`interface-number`: Specifies a Layer 2 aggregate interface number. The value range for the *`interface-number`* argument is 1 to 1024.

Usage guidelines

When you create a Layer 2 aggregate interface, the system automatically creates a Layer 2 aggregation group with the same number. The aggregation group operates in static aggregation mode by default.

Deleting a Layer 2 aggregate interface also deletes the Layer 2 aggregation group. At the same time, the member ports of the aggregation group, if any, leave the aggregation group.

Examples

Create Layer 2 aggregate interface Bridge-Aggregation 1, and enter its view.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1]
```

jumboframe enable

Use **jumboframe enable** to allow the jumbo frames on an interface to pass through.

Use **undo jumboframe enable** to deny jumbo frames on an interface.

Use **undo jumboframe enable** *size* to restore the default.

Syntax

jumboframe enable [*size*]

undo jumboframe enable [*size*]

Default

An interface allows jumbo frames with a maximum length of 10240 bytes to pass through.

Views

Layer 2 aggregate interface view

Predefined user roles

network-admin

size: Specifies the maximum length of jumbo frames, in bytes. The value range for this argument is 1522 to 10240.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Allow jumbo frames on Layer 2 aggregate interface Bridge-Aggregation 1.

```
<Sysname> System-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] jumboframe enable
```

lacp default-selected-port disable

Use **lacp default-selected-port disable** to disable the default port selection action for dynamic aggregation groups.

Use **undo lacp default-selected-port disable** to enable the default port selection action for dynamic aggregation groups.

Syntax

lacp default-selected-port disable

undo lacp default-selected-port disable

Default

The default port selection action is enabled for dynamic aggregation groups.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The default port selection action applies to dynamic aggregation groups.

This action automatically chooses the port with the lowest ID from among all up member ports as a Selected port if none of them has received LACPDUs before the LACP timeout interval expires.

After this action is disabled, a dynamic aggregation group will not have any Selected ports to forward traffic if it has not received LACPDUs before the LACP timeout interval expires.

Examples

Disable the default port selection action.

```
<Sysname> system-view
[Sysname] lacp default-selected-port disable
```

lacp edge-port

Use **lacp edge-port** to configure an aggregate interface as an edge aggregate interface.

Use **undo lacp edge-port** to restore the default.

Syntax

lacp edge-port

undo lacp edge-port

Default

An aggregate interface does not operate as an edge aggregate interface.

Views

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

Use this command on the aggregate interface that connects the device to a server if dynamic link aggregation is configured only on the device. This feature improves link reliability by enabling all member ports of the aggregation group to forward packets.

This command takes effect only on an aggregate interface corresponding to a dynamic aggregation group.

Link-aggregation traffic redirection cannot operate correctly on an edge aggregate interface.

Examples

Configure Layer 2 aggregate interface Bridge-Aggregation 1 as an edge aggregate interface.

```
<Sysname> System-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] lacp edge-port
```

lacp mode

Use **lacp mode passive** to configure LACP to operate in passive mode on a port.

Use **undo lacp mode** to restore the default.

Syntax

lacp mode passive

undo lacp mode

Default

LACP operates in active mode on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only on member ports of dynamic aggregation groups.

When LACP is operating in passive mode on a local member port and its peer port, both ports cannot send LACPDUs. When LACP is operating in active mode on either end of a link, both ports can send LACPDUs.

Examples

Configure LACP to operate in passive mode on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lacp mode passive
```

lacp period short

Use **lacp period short** to enable the short LACP timeout interval (3 seconds) on an interface.

Use **undo lacp period** to restore the default.

Syntax

lacp period short

undo lacp period

Default

The LACP timeout interval is the long timeout interval (90 seconds) on an interface.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Examples

Enable the short LACP timeout interval (3 seconds) on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lacp period short
```

lacp select speed

Use **lacp select speed** to configure a dynamic aggregation group to use port speed as the prioritized criterion for reference port selection.

Use **undo lacp select speed** to restore the default.

IMPORTANT:

This feature is supported only in Release 6348P01 and later versions.

Syntax

lacp select speed

undo lacp select speed

Default

Port ID is the prioritized criterion for reference port selection in a dynamic aggregation group.

Views

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

CAUTION:

Changing reference port selection criteria might cause transient traffic interruption. When you use this command, make sure you understand its impact on your network.

This command enables a dynamic aggregation group to select a high-speed member port as the reference port.

You must execute this command at both ends of the aggregate link so the peer aggregation systems use the same criteria for reference port selection.

As a best practice, shut down the peer aggregate interfaces before you execute this command and bring up the interfaces after this command is executed on both of them.

This command takes effect only on dynamic aggregate interfaces. On a static aggregate interface, you can execute this command, but the setting cannot take effect.

Examples

Specify port speed as the prioritized criterion for reference port selection on Layer 2 dynamic aggregate interface Bridge-Aggregation 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
```

```
[Sysname-Bridge-Aggregation1] link-aggregation mode dynamic
[Sysname-Bridge-Aggregation1] lacp select speed
```

lacp system-mac

Use **lacp system-mac** to set the LACP system MAC address.

Use **undo lacp system** to restore the default.

Syntax

lacp system-mac *mac-address*

undo lacp system-mac

Default

The LACP system MAC address is the bridge MAC address of the device.

Views

System view

Predefined user roles

network-admin

Parameters

mac-address: Specifies a MAC address in the format of H-H-H. The MAC address cannot be an all-zero, all-F, or multicast MAC address.

Usage guidelines

All S-MLAG devices must use the same LACP system MAC address.

The LACP system MAC address configured by using this command takes effect only on aggregate interfaces in S-MLAG groups. Aggregate interfaces not in S-MLAG groups do not use the configured LACP system MAC address to send LACPDUs. To identify the LACP system MAC address used by a link aggregation group, examine the **System ID** field in the output from the **display link-aggregation verbose** command.

Examples

Set the LACP system MAC address to **0001-0001-0001**.

```
<Sysname> system-view
[Sysname] lacp system-mac 1-1-1
```

Related commands

display link-aggregation verbose

lacp system-number

Use **lacp system-number** to set the LACP system number used by the local device.

Use **undo lacp system-number** to restore the default.

Syntax

lacp system-number *number*

undo lacp system-number

Default

The LACP system number is not set.

Views

System view

Predefined user roles

network-admin

Parameters

number: Specifies a number in the range of 1 to 3.

Usage guidelines

You must assign a unique LACP system number to each S-MLAG device.

The LACP system number configured by using this command takes effect only on aggregate interfaces in S-MLAG groups. Aggregate interfaces not in S-MLAG groups do not use the configured LACP system number in LACPDUs. To view the LACP system number in LACPDUs, examine the **Index** field in the output from the **display link-aggregation verbose** command.

Examples

Set the LACP system number to 1.

```
<Sysname> system-view
[Sysname] lacp system-number 1
```

Related commands

display link-aggregation verbose

lacp system-priority

Use **lacp system-priority** to set the LACP system priority.

Use **undo lacp system-priority** to restore the default.

Syntax

lacp system-priority *priority*

undo lacp system-priority

Default

The LACP system priority is 32768.

Views

System view

Predefined user roles

network-admin

Parameters

priority: Specifies the LACP system priority in the range of 0 to 65535. The smaller the value, the higher the LACP system priority.

Usage guidelines

All S-MLAG devices must use the same LACP system priority.

Examples

Set the LACP system priority to 64.

```
<Sysname> system-view
[Sysname] lacp system-priority 64
```

Related commands

link-aggregation port-priority

link-aggregation bfd ipv4

Use **link-aggregation bfd ipv4** to enable BFD for an aggregation group.

Use **undo link-aggregation bfd** to disable BFD for an aggregation group.

Syntax

link-aggregation bfd ipv4 source *ip-address* **destination** *ip-address*

undo link-aggregation bfd

Default

BFD is disabled for an aggregation group.

Views

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

source *ip-address*: Specifies the unicast source IP address of BFD sessions. The source IP address cannot be 0.0.0.0.

destination *ip-address*: Specifies the unicast destination IP address of BFD sessions. The destination IP address cannot be 0.0.0.0.

Usage guidelines

Make sure the source and destination IP addresses are reversed between the two ends of an aggregate link. For example, if you execute **link-aggregation bfd ipv4 source 1.1.1.1 destination 2.2.2.2** at the local end, execute **link-aggregation bfd ipv4 source 2.2.2.2 destination 1.1.1.1** at the peer end. The source and destination IP addresses cannot be the same.

The BFD parameters configured on an aggregate interface take effect on all BFD sessions established by the member ports in its aggregation group. BFD on an aggregate link supports only control packet mode for session establishment and maintenance. The two ends of an established BFD session can only operate in Asynchronous mode. For more information about BFD, see *High Availability Configuration Guide*.

As a best practice, do not configure BFD for any protocols on a BFD-enabled aggregate interface.

Make sure the number of member ports in the BFD-enabled aggregation group is less than or identical to the number of BFD sessions supported by the device. If the aggregation group contains more member ports than the supported sessions, some Selected ports might change to the Unselected state.

If the number of BFD sessions differs between the two ends of an aggregate link, check their settings for inconsistency in the maximum number of Selected ports. You must make sure the two ends have the same setting for the maximum number of Selected ports.

Examples

Enable BFD for Layer 2 aggregation group 1, and specify the source and destination IP addresses as 1.1.1.1 and 2.2.2.2 for BFD sessions.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
```

```
[Sysname-Bridge-Aggregation1] link-aggregation bfd ipv4 source 1.1.1.1 destination
2.2.2.2
```

link-aggregation global load-sharing mode

Use **link-aggregation global load-sharing mode** to set the global link-aggregation load sharing mode.

Use **undo link-aggregation global load-sharing mode** to restore the default.

Syntax

link-aggregation global load-sharing mode { **destination-ip** | **destination-mac** | **destination-port** | **ingress-port** | **source-ip** | **source-mac** | **source-port** } *

undo link-aggregation global load-sharing mode

Default

Packets are load shared based on the following information:

- Source and destination IP addresses.
- Source and destination MAC addresses.

Views

System view

Predefined user roles

network-admin

Parameters

destination-ip: Distributes traffic based on destination IP addresses.

destination-mac: Distributes traffic based on destination MAC addresses.

destination-port: Distributes traffic based on destination ports.

ingress-port: Distributes traffic based on ingress ports.

source-ip: Distributes traffic based on source IP addresses.

source-mac: Distributes traffic based on source MAC addresses.

source-port: Distributes traffic based on source ports.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

If an unsupported load sharing mode is set, the device displays an error message.

The following are global load sharing modes supported on the device:

- Default mode (load sharing mode automatically determined based on the packet type).
- Source IP.
- Destination IP.
- Source MAC.
- Destination MAC.
- Ingress port.
- Source IP and destination IP.
- Source IP and source port.

- Destination IP and destination port.
- Source IP, source port, destination IP, and destination port.
- Any combinations of ingress port, source MAC, and destination MAC.

Examples

Set the global load sharing mode to load share packets based on destination MAC addresses.

```
<Sysname> system-view
[Sysname] link-aggregation global load-sharing mode destination-mac
```

link-aggregation lacp traffic-redirect-notification enable

Use **link-aggregation lacp traffic-redirect-notification enable** to enable link-aggregation traffic redirection.

Use **undo link-aggregation lacp traffic-redirect-notification enable** to disable link-aggregation traffic redirection.

Syntax

link-aggregation lacp traffic-redirect-notification enable

undo link-aggregation lacp traffic-redirect-notification enable

Default

Link-aggregation traffic redirection is disabled.

Views

System view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

This feature redirects traffic on a Selected port to the remaining available Selected ports of an aggregation group if one of the following events occurs:

- The port is shut down by using the **shutdown** command.
- The slot that hosts the port reboots, and the aggregation group spans multiple slots.

NOTE:

The device does not redirect traffic to member ports that become Selected during the traffic redirection process.

This feature ensures zero packet loss for known unicast traffic, but does not protect unknown unicast traffic.

This feature applies only to dynamic link aggregation groups.

To prevent traffic interruption, enable link-aggregation traffic redirection on devices at both ends of the aggregate link.

To prevent packet loss that might occur when a slot reboots, do not enable spanning tree together with link-aggregation traffic redirection.

Link-aggregation traffic redirection cannot operate correctly on an edge aggregate interface.

Global link-aggregation traffic redirection settings take effect on all aggregation groups. A link aggregation group preferentially uses the group-specific link-aggregation traffic redirection settings.

If group-specific link-aggregation traffic redirection is not configured, the group uses the global link-aggregation traffic redirection settings.

As a best practice, enable link-aggregation traffic redirection on a per-interface basis. If you enable this feature globally, communication with a third-party peer device might be affected if the peer is not compatible with this feature.

Examples

Enable link-aggregation traffic redirection.

```
<Sysname> system-view
[Sysname] link-aggregation lacp traffic-redirect-notification enable
```

link-aggregation load-sharing mode local-first

Use **link-aggregation load-sharing mode local-first** to enable local-first load sharing for link aggregation.

Use **undo link-aggregation load-sharing mode local-first** to disable local-first load sharing for link aggregation.

Syntax

link-aggregation load-sharing mode local-first

undo link-aggregation load-sharing mode local-first

Default

Local-first load sharing is enabled for link aggregation.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Use local-first load sharing in a multidevice link aggregation scenario to distribute traffic preferentially across member ports on the ingress device. Local-first load sharing takes effect only on known unicast traffic.

If you disable local-first load sharing, packets of an aggregate interface are load shared among all Selected ports on IRF member devices.

Examples

Disable local-first load sharing for link aggregation.

```
<Sysname> system-view
[Sysname] undo link-aggregation load-sharing mode local-first
```

link-aggregation mode

Use **link-aggregation mode dynamic** to configure an aggregation group to operate in dynamic aggregation mode and enable LACP.

Use **undo link-aggregation mode** to restore the default.

Syntax

link-aggregation mode dynamic

undo link-aggregation mode

Default

An aggregation group operates in static aggregation mode.

Views

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

When you change the aggregation mode, make sure you understand the impact of the change on services.

Aggregation mode change might cause Selected member ports to become Unselected.

Examples

Configure Layer 2 aggregation group 1 to operate in dynamic aggregation mode.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] link-aggregation mode dynamic
```

link-aggregation port-priority

Use **link-aggregation port-priority** to set the port priority of an interface.

Use **undo link-aggregation port-priority** to restore the default.

Syntax

link-aggregation port-priority *priority*

undo link-aggregation port-priority

Default

The port priority of an interface is 32768.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

priority: Specifies the port priority in the range of 0 to 65535. The smaller the value, the higher the port priority.

Examples

Set the port priority to 64 for Layer 2 Ethernet interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] link-aggregation port-priority 64
```

Related commands

lacp system-priority

link-aggregation selected-port maximum

Use **link-aggregation selected-port maximum** to set the maximum number of Selected ports allowed in an aggregation group.

Use **undo link-aggregation selected-port maximum** to restore the default.

Syntax

link-aggregation selected-port maximum *max-number*

undo link-aggregation selected-port maximum

Default

The maximum number of Selected ports allowed in an aggregation group is 8.

Views

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

max-number: Specifies the maximum number of Selected ports allowed in an aggregation group. The value range for this argument is 1 to 8.

Usage guidelines

Executing this command might cause some of the Selected ports in an aggregation group to become Unselected ports.

The maximum number of Selected ports allowed in the aggregation groups must be the same for the local and peer ends.

For an aggregation group, the maximum number of Selected ports must be equal to or higher than the minimum number of Selected ports.

The maximum number of Selected ports allowed in an aggregation group is limited by one of the following values, whichever value is smaller:

- Maximum number set by using the **link-aggregation selected-port maximum** command.
- Maximum number of Selected ports allowed by the link aggregation capability.

You can implement backup between two ports by performing the following tasks:

- Assigning two ports to an aggregation group.
- Setting the maximum number of Selected ports to 1 for the aggregation group.

Then, only one Selected port is allowed in the aggregation group at any point in time, while the Unselected port acts as a backup port.

Examples

Set the maximum number of Selected ports to 5 for Layer 2 aggregation group 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] link-aggregation selected-port maximum 5
```

Related commands

link-aggregation selected-port minimum

link-aggregation selected-port minimum

Use **link-aggregation selected-port minimum** to set the minimum number of Selected ports in an aggregation group.

Use **undo link-aggregation selected-port minimum** to restore the default.

Syntax

link-aggregation selected-port minimum { *min-number* | **percentage** *number* }

undo link-aggregation selected-port minimum

Default

The minimum number of Selected ports in an aggregation group is not specified.

Views

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

min-number: Specifies the minimum number of Selected ports in an aggregation group required to bring up the aggregate interface. The value range for this argument is 1 to 8.

percentage *number*: Sets the minimum percentage of Selected ports in an aggregation group. The value range for the *number* argument is 1 to 100.

Usage guidelines

IMPORTANT:

After you set the minimum percentage of Selected ports for an aggregation group, aggregate interface flapping might occur when ports join or leave an aggregation group. Make sure you are fully aware of the impacts of this setting when you configure it on a live network.

You can set either the minimum number or the minimum percentage of Selected ports for an aggregation group. If you configure both settings on an aggregate interface, the higher Selected port number limit takes effect.

Executing this command might cause all member ports in the aggregation group to become Unselected ports.

You must set the same minimum number or minimum percentage of Selected ports at the two ends of an aggregate link.

For an aggregation group, the minimum number of Selected ports must be equal to or lower than the maximum number of Selected ports.

Examples

Set the minimum number of Selected ports to 3 for Layer 2 aggregation group 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] link-aggregation selected-port minimum 3
```

Related commands

link-aggregation selected-port maximum

link-delay

Use **link-delay** to set the physical state change suppression interval on an aggregate interface.

Use **undo link-delay** to restore the default.

Syntax

link-delay { **down** | **up** } [**msec**] *delay-time*

undo link-delay { **down** | **up** }

Default

Each time the physical link of an aggregate interface goes up or comes down, the system immediately reports the change to the CPU.

Views

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

down: Suppresses the link-down events.

up: Suppresses the link-up events.

msec: Sets the physical state change suppression interval in milliseconds. If you do not specify this keyword, the suppression interval is in seconds.

delay-time: Sets the physical state change suppression interval. To report a physical state change immediately to the CPU, set the interval to 0.

- If you do not specify the **msec** keyword, the value range is 0 to 30 seconds.
- If you specify the **msec** keyword, the value range is 0 to 10000 milliseconds, and the value must be a multiple of 100.

Usage guidelines

You can configure this feature to suppress link-down events, link-up events, or both. If an event of the specified type still exists when the suppression interval expires, the system reports the event.

On an interface, you can configure different suppression intervals for link-up and link-down events. If you execute the **link-delay** command multiple times for an event type, the most recent configuration takes effect on that event type.

Do not use this feature in combination with S-MLAG.

When you use this feature on an aggregate interface, make sure its peer is also an aggregate interface. In addition, you must set the physical state change suppression interval to the same value on those aggregate interfaces.

Examples

Set the link-down event suppression interval to 8 seconds on Bridge-Aggregation 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] link-delay down 8
```

port link-aggregation group

Use **port link-aggregation group** to assign an interface to an aggregation group.

Use **undo port link-aggregation group** to remove an interface from the aggregation group to which it belongs.

Syntax

port link-aggregation group { *group-id* [**force**] | **auto** [*group-id*] }

undo port link-aggregation group

Default

An interface does not belong to any aggregation group.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

group-id: Specifies an aggregation group by its aggregate interface number. The value range for the *number* argument is 1 to 1024.

force: Enables the current interface to synchronize attribute configurations from the aggregate interface. If you do not specify this keyword, the current interface does not synchronize attribute configurations from the aggregate interface when it joins the aggregation group.

auto: Enables automatic assignment.

Usage guidelines

An interface can belong to only one aggregation group.

An interface cannot join an aggregation group if it has different attribute configurations from the aggregate interface. After joining an aggregation group, an interface inherits the attribute configurations on the aggregate interface. You can modify the attribute configurations only on the aggregate interface.

The **force** keyword takes effect only when you assign the interface to an aggregation group. It cannot be saved in the running configuration or a configuration file.

When you enable automatic assignment, you can specify a preferred aggregation group, which must be in dynamic mode.

The device assigns the interface to the preferred aggregation group as long as the LACPDUs received on the interface match the peer information of the reference port in the group.

If you do not specify a preferred group or if the preferred group match fails, the device attempts to select a matching group from the existing dynamic aggregation groups. If no match is found, the device creates a dynamic aggregation group based on the LACPDUs and assigns the interface to that aggregation group.

As a best practice, do not modify the configuration on an automatically created aggregate interface or its member ports.

Examples

Assign Layer 2 Ethernet interface GigabitEthernet 1/0/1 to Layer 2 aggregation group 1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-aggregation group 1
```

port s-mlag group

Use **port s-mlag group** to assign an aggregate interface to an S-MLAG group.

Use **undo port s-mlag group** to restore the default.

Syntax

port s-mlag group *group-id*

undo port s-mlag group

Default

An aggregate interface is not in any S-MLAG group.

Views

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

group-id: Specifies an S-MLAG group number in the range of 1 to 1024.

Usage guidelines

Use S-MLAG to set up link aggregations only with servers.

You can assign only Layer 2 aggregate interfaces in dynamic mode to an S-MLAG group.

Each S-MLAG group can contain only one aggregate interface on each device.

Examples

Assign Bridge-Aggregation 1 to S-MLAG group 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port s-mlag group 1
```

reset counters interface

Use **reset counters interface** to clear statistics for the specified aggregate interfaces.

Syntax

reset counters interface [**bridge-aggregation** [*interface-number*]]

Views

User view

Predefined user roles

network-admin

Parameters

bridge-aggregation: Specifies Layer 2 aggregate interfaces.

interface-number: Specifies an existing aggregate interface number.

Usage guidelines

Use this command to clear history statistics before you collect traffic statistics for a time period.

If you do not specify an aggregate interface type, the command clears statistics for all interfaces in the system.

If you specify only an aggregate interface type, the command clears statistics for all aggregate interfaces of the specified type.

The **bridge-aggregation** keyword is available only when Layer 2 aggregate interfaces exist on the device.

Examples

Clear statistics for Layer 2 aggregate interface Bridge-Aggregation 1.

```
<Sysname> reset counters interface bridge-aggregation 1
```

reset lacp statistics

Use **reset lacp statistics** to clear LACP statistics for the specified link aggregation member ports.

Syntax

reset lacp statistics [**interface** *interface-list*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-list*: Specifies a list of link aggregation member ports, in the format *interface-type interface-number1* [**to** *interface-type interface-number2*]. The value for the *interface-number1* argument must be equal to or greater than the value for the *interface-number2* argument. If you do not specify any member ports, the command clears LACP statistics for all member ports.

Examples

Clear LACP statistics for all link aggregation member ports.

```
<Sysname> reset lacp statistics
```

Related commands

display link-aggregation member-port

shutdown

Use **shutdown** to shut down an aggregate interface.

Use **undo shutdown** to bring up an aggregate interface.

Syntax

shutdown

undo shutdown

Views

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

CAUTION:

The **shutdown** command will disconnect all links established on an interface. Make sure you are fully aware of the impacts of this command when you use it on a live network.

Examples

Bring up Layer 2 aggregate interface Bridge-Aggregation 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] undo shutdown
```

Contents

Port isolation commands

display port-isolate group

Use **display port-isolate group** to display port isolation group information.

Syntax

display port-isolate group [*group-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group-id: Specifies an isolation group by its ID. The value range is 1 to 8.

Examples

Display all isolation groups.

```
<Sysname> display port-isolate group
 Port isolation group information:
 Group ID: 1
 Group members:
    GigabitEthernet1/0/1

 Group ID: 5
 Group members:
    GigabitEthernet1/0/2            GigabitEthernet1/0/4
```

Display information about isolation group 1.

```
<Sysname> display port-isolate group 1
 Port isolation group information:
 Group ID: 1
 Group members:
    GigabitEthernet1/0/1
```

Table 1 Command output

Field	Description
Group ID	ID of the isolation group.
Group members	Isolated ports in the isolation group. **No ports** indicates that the isolation group does not contain isolated ports.

Related commands

port-isolate enable

port-isolate enable

Use **port-isolate enable** to assign a port to an isolation group.

Use **undo port-isolate enable** to remove a port from an isolation group.

Syntax

port-isolate enable group *group-id*

undo port-isolate enable

Default

The port is not assigned to an isolation group.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

group *group-id*: Specifies an isolation group by its ID. The value range is 1 to 8.

Usage guidelines

The configuration in Layer 2 Ethernet interface view applies only to the interface.

The configuration in Layer 2 aggregate interface view applies to the Layer 2 aggregate interface and its aggregation member ports. If the device fails to apply the configuration to the aggregate interface, it does not assign any aggregation member port to the isolation group. If the failure occurs on an aggregation member port, the device skips the port and continues to assign other aggregation member ports to the isolation group.

To assign ports to an isolation group, make sure the isolation group already exists.

One port can be assigned to only one isolation group.

Examples

Assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to isolation group 1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-isolate enable group 1
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] port-isolate enable group 1
```

Related commands

display port-isolate group

port-isolate group

Use **port-isolate group** to create an isolation group.

Use **undo port-isolate group** to delete isolation groups.

Syntax

port-isolate group *group-id*

undo port-isolate group { *group-id* | **all** }

Default

No isolation groups exist.

Views

System view

Predefined user roles

network-admin

Parameters

group-id: Specifies an isolation group by its ID. The value range is 1 to 8.

all: Deletes all isolation groups.

Examples

Create isolation group 1.

```
<Sysname> system-view
[Sysname] port-isolate group 1
```

Contents

Spanning tree commands

active region-configuration

Use **active region-configuration** to activate your MST region configuration.

Syntax

active region-configuration

Views

MST region view

Predefined user roles

network-admin

Usage guidelines

When you configure MST region parameters, MSTP launches a new spanning tree calculation process that might cause network topology instability. This is most likely to occur when you configure the VLAN-to-instance mapping table. The launch occurs after you execute the **active region-configuration** command or the **stp global enable** command.

As a best practice, use the **check region-configuration** command to determine whether the MST region configurations to be activated are correct. Run this command only when they are correct.

Examples

Map VLAN 2 to MSTI 1 and activate the MST region configuration.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] instance 1 vlan 2
[Sysname-mst-region] active region-configuration
```

Related commands

check region-configuration

instance

region-name

revision-level

stp global enable

vlan-mapping modulo

bpdu-drop any

Use **bpdu-drop any** to enable BPDU drop on a port.

Use **undo bpdu-drop any** to disable BPDU drop on a port.

Syntax

bpdu-drop any

undo bpdu-drop any

Default

BPDU drop is disabled on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Examples

Enable BPDU drop on port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] bpdu-drop any
```

check region-configuration

Use **check region-configuration** to display MST region pre-configuration information.

Syntax

check region-configuration

Views

MST region view

Predefined user roles

network-admin

Usage guidelines

Spanning tree devices belong to the same MST region only when they are connected through a physical link and configured with the same details as follows:

- Format selector (0 by default and not configurable).
- MST region name.
- MST region revision level.
- VLAN-to-instance mapping entries in the MST region.

As a best practice, use this command to determine whether the MST region configurations to be activated are correct. Activate them only when they are correct.

Examples

Display MST region pre-configurations.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] check region-configuration
 Admin Configuration
   Format selector      : 0
   Region name          : 001122334400
   Revision level       : 0
   Configuration digest : 0x3ab68794d602fdf43b21c0b37ac3bca8

   Instance  VLANs Mapped
   0         1, 3 to 4094
```

15 2

Table 1 Command output

Field	Description
Format selector	Format selector of the MST region, which is 0 (not configurable).
Region name	MST region name.
Revision level	Revision level of the MST region.
Instance VLANs Mapped	VLAN-to-instance mappings in the MST region.

Related commands

active region-configuration

instance

region-name

revision-level

vlan-mapping modulo

display stp

Use **display stp** to display spanning tree status and statistics.

Syntax

display stp [**instance** *instance-list* | **vlan** *vlan-id-list*] [**interface** *interface-list* | **slot** *slot-number*] [**brief**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

interface *interface-list*: Specifies a space-separated list of up to 10 interface items. Each item specifies an interface or a range of interfaces in the form of *interface-type interface-number 1* [**to** *interface-type interface-number 2*]. The interface number for *interface-number 2* must be equal to or greater than the interface number for *interface-number 1*.

brief: Displays brief spanning tree status and statistics. If this keyword is not specified, the command displays detailed spanning tree status and statistics.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices.

Usage guidelines

In STP or RSTP mode, the command output is sorted by port name.

- If you do not specify a port, this command applies to all ports.
- If you specify a port list, this command applies to the specified ports.

In PVST mode, the command output is sorted by VLAN ID and by port name in each VLAN.

- If you do not specify a VLAN or port, this command applies to all ports in all VLANs.
- If you only specify a VLAN list but not a port, this command applies to all ports in the specified VLANs.
- If you only specify a port list but not a VLAN, this command applies to the specified ports in all VLANs.
- If you specify both a VLAN list and a port list, this command applies to the ports in the specified VLANs.

In MSTP mode, the command output is sorted by MSTI ID and by port name in each MSTI.

- If you do not specify an MSTI or port, this command applies to all MSTIs on all ports.
- If you specify an MSTI list but not a port, this command applies to all ports in the specified MSTIs.
- If you specify a port list but not an MSTI, this command applies to all MSTIs on the specified ports.
- If you specify both an MSTI list and a port list, this command applies to the specified ports in the specified MSTIs.

Examples

In MSTP mode, display the brief spanning tree status and statistics for MSTI 0 on port GigabitEthernet 1/0/1.

```
<Sysname> display stp instance 0 interface GigabitEthernet 1/0/1 brief
 MST ID      Port                        Role  STP State     Protection
 0           0           GigabitEthernet1/0/1         ALTE  DISCARDING    LOOP
```

In PVST mode, display the brief spanning tree status and statistics for VLAN 2 on port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] display stp vlan 2 interface gigabitethernet 1/0/1 brief
 VLAN ID     Port                        Role  STP State     Protection
 2           GigabitEthernet1/0/1        ALTE  DISCARDING    LOOP
```

Table 2 Command output

Field	Description
MST ID	MSTI ID in the MST region.
Port	Port name, corresponding to each MSTI or VLAN.
Role	Port role: • **ALTE**—The port is an alternate port. • **BACK**—The port is a backup port. • **ROOT**—The port is a root port. • **DESI**—The port is a designated port. • **MAST**—The port is a master port.

Field	Description
	• **DISA**—The port is disabled.
STP State	Spanning tree status on the port: • **FORWARDING**—The port can receive and send BPDUs and also forward user traffic. • **DISCARDING**—The port can receive and send BPDUs but cannot forward user traffic. • **LEARNING**—The port is in a transitional state. It can receive and send BPDUs but cannot forward user traffic.
Protection	Effective spanning tree protection feature on the port: • **ROOT**—Root guard. • **LOOP**—Loop guard. • **BPDU**—BPDU guard. If no spanning tree protection feature is configured or spanning tree protection is not triggered, this field displays **NONE**.

In MSTP mode, display the detailed spanning tree status and statistics for all MSTIs on all ports.

```
<Sysname> display stp
-------[CIST Global Info][Mode MSTP]-------
 Bridge ID           : 32768.0001-0000-0000
 Bridge times        : Hello 2s MaxAge 20s FwdDelay 15s MaxHops 20
 Root ID/ERPC        : 32768.0001-0000-0000, 0
 RegRoot ID/IRPC     : 32768.0001-0000-0000, 0
 RootPort ID         : 0.0
 BPDU-Protection     : Disabled
 Bridge Config-
 Digest-Snooping     : Disabled
 TC or TCN received  : 2
 Time since last TC  : 0 days 0h:0m:58s

----[Port1(GigabitEthernet1/0/1)][FORWARDING]----
 Port protocol       : Enabled
 Port role           : Designated Port (Boundary)
 Port ID             : 128.3
 Port cost(Legacy)   : Config=auto, Active=200
 Desg.bridge/port    : 32768.0001-0000-0000, 128.3
 Port edged          : Config=disabled, Active=disabled
 Point-to-Point      : Config=auto, Active=true
 Transmit limit      : 10 packets/hello-time
 TC-Restriction      : Disabled
 Role-Restriction    : Disabled
 Protection type     : Config=none, Active=none
 MST BPDU format     : Config=auto, Active=802.1s
 Port Config-
 Digest-Snooping     : Disabled
 Rapid transition    : True
 Num of VLANs mapped : 0
 Port times          : Hello 2s MaxAge 20s FwdDelay 15s MsgAge 0s RemHops 20
 BPDU sent           : 32
```

```
          TCN: 0, Config: 0, RST: 0, MST: 32
 BPDU received       : 2
          TCN: 0, Config: 0, RST: 0, MST: 2

-------[MSTI 1 Global Info]-------
 Bridge ID           : 32768.0001-0000-0000
 RegRoot ID/IRPC     : 32768.0001-0000-0000, 0
 RootPort ID         : 0.0
 Master bridge       : 32768.0001-0000-0000
 Cost to master      : 0
 TC received         : 0

----[Port1(GigabitEthernet1/0/1)][FORWARDING]----
 Port protocol       : Enabled
 Port role           : Designated Port (Boundary)
 Port ID             : 128.3
 Port cost(Legacy)   : Config=auto, Active=200
 Desg.bridge/port    : 32768.0001-0000-0000, 128.3
 Protection type     : Config=none, Active=none
 Rapid transition    : True
 Num of VLANs mapped : 64
 Port times          : RemHops 20
```

In PVST mode, display the spanning tree status and statistics for all ports in all VLANs.

```
<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] display stp
-------[VLAN 1 Global Info]-------
Protocol status     : Enabled
Bridge ID           : 32768.000f-e200-2200
Bridge times        : Hello 2s MaxAge 20s FwdDelay 15s
VlanRoot ID/RPC     : 0.00e0-fc0e-6554, 200200
RootPort ID         : 128.48
BPDU-Protection     : Disabled
TC or TCN received  : 2
Time since last TC  : 0 days 0h:5m:42s

 ----[Port1(GigabitEthernet1/0/1)][FORWARDING]----
 Port protocol       : Enabled
 Port role           : Designated Port
 Port ID             : 128.153
 Port cost(Legacy)   : Config=auto, Active=200
 Desg. bridge/port   : 32768.000f-e200-2200, 128.2
 Port edged          : Config=disabled, Active=disabled
 Point-to-Point      : Config=auto, Active=true
 Transmit limit      : 10 packets/hello-time
 Protection type     : Config=none, Active=none
 Rapid transition    : False
 Port times          : Hello 2s MaxAge 20s FwdDelay 15s MsgAge 2s
```

```
-------[VLAN 2 Global Info]-------
Protocol status      : Enabled
Bridge ID            : 32768.000f-e200-2200
Bridge times         : Hello 2s MaxAge 20s FwDly 15s
VlanRoot ID/RPC      : 0.00e0-fc0e-6554, 200200
RootPort ID          : 128.48
BPDU-Protection      : Disabled
TC or TCN received   : 2
Time since last TC   : 0 days 0h:5m:42s
```

In MSTP mode, display the spanning tree status and statistics when the spanning tree feature is disabled.

```
<Sysname> display stp
 Protocol status    : Disabled
 Protocol Std.      : IEEE 802.1s
 Version            : 3
 Bridge-Prio.       : 32768
 MAC address        : 000f-e200-8048
 Max age(s)         : 20
 Forward delay(s)   : 15
 Hello time(s)      : 2
 Max hops           : 20
 TC Snooping        : Disabled
```

In PVST mode, display the spanning tree status and statistics when the spanning tree feature is disabled.

```
<Sysname> display stp
 Protocol status    : Disabled
 Protocol Std.      : IEEE 802.1w (pvst)
 Version            : 2
 Bridge-Prio.       : 32768
 MAC address        : 3822-d69f-0800
 Max age(s)         : 20
 Forward delay(s)   : 15
 Hello time(s)      : 2
 TC Snooping        : Disabled
```

Table 3 Command output

Field	Description
Bridge ID	Bridge ID, which contains the device's priority and its MAC address. For example, in output 32768.000f-e200-2200, the value preceding the dot is the device's priority. The value following the dot is the device's MAC address.
Bridge times	Major parameters for the bridge: • **Hello**—Hello timer. • **MaxAge**—Maximum age timer. • **FwdDelay**—Forward delay timer. • **MaxHops**—Maximum hops within the MST region.
Root ID/ERPC	CIST root ID and external path cost (the path cost from the device to the CIST root).
RegRoot ID/IRPC	CIST regional root ID and internal path cost (the path cost from the device to the

Field	Description
	CIST regional root).
VlanRoot ID/RPC	VLAN root ID and root path cost (the path cost from the device to the VLAN root bridge).
RootPort ID	Root port ID. The value **0.0** indicates that the device is the root and there is no root port.
BPDU-Protection	Global status of the BPDU guard feature.
Bridge Config-Digest-Snooping	Global status of Digest Snooping.
TC or TCN received	Number of TC/TCN BPDUs received in the MSTI or VLAN.
Time since last TC	Time since the latest topology change in the MSTI or VLAN.
[FORWARDING]	The port is in forwarding state.
[DISCARDING]	The port is in discarding state.
[LEARNING]	The port is in learning state.
Port protocol	Status of the spanning tree feature on the port.
Port role	Port role: • Alternate. • Backup. • Root. • Designated. • Master. • Disabled.
(Boundary)	The port is a regional boundary port.
Port cost(Legacy)	Path cost of the port. The field in parentheses indicates the standard (legacy, dot1d-1998, or dot1t) used for port path cost calculation. • **Config**—Configured value. • **Active**—Actual value.
Desg.bridge/port	Designated bridge ID and port ID of the port. The port ID displayed is insignificant for a port which does not support port priority.
Port edged	The port is an edge port or non-edge port. • **Config**—Configured value. • **Active**—Actual value.
Point-to-Point	The port is connected to a point-to-point link or not. • **Config**—Configured value. • **Active**—Actual value.
Transmit limit	Maximum number of BPDUs sent by a port within each hello time.
Protection type	Whether spanning tree protection is configured on the port: • **Config**—Configured spanning tree protection feature. • **Active**—Effective spanning tree protection feature. Spanning tree protection features are as follows: • **ROOT**—Root guard. • **LOOP**—Loop guard. • **BPDU**—BPDU guard. • **PVST BPDU**—PVST BPDU guard. If no spanning tree protection feature is configured or spanning tree protection is not

Field	Description
	triggered, this field displays **NONE**.
TC-Restriction	Status of TC transmission restriction on the port.
Role-Restriction	Status of port role restriction on the port.
MST BPDU format	Format of the MST BPDUs that the port can send: • **Config**—Configured value (legacy or 802.1s). • **Active**—Actual value (legacy or 802.1s).
Port Config-Digest-Snooping	Status of Digest Snooping on the port.
Rapid transition	Indicates whether the port rapidly transits to the forwarding state in the MSTI or VLAN.
Num of VLANs mapped	Number of VLANs that are mapped to the MSTI.
Port times	Major parameters for the port: • **Hello**—Hello timer. • **MaxAge**—Maximum age timer. • **FwdDelay**—Forward delay timer. • **MsgAge**—Message age timer. • **RemHops**—Remaining hops.
BPDU sent	Statistics on sent BPDUs.
BPDU received	Statistics on received BPDUs.
RegRoot ID/IRPC	MSTI regional root/internal path cost.
Root Type	MSTI root type: • **Primary root**. • **Secondary root**.
Master bridge	MSTI root bridge ID.
Cost to master	Path cost from the MSTI to the master bridge.
TC received	Number of received TC BPDUs.
Protocol status	Spanning tree protocol status.
Protocol Std.	Spanning tree protocol standard.
Version	Spanning tree protocol version.
Bridge-Prio.	In MSTP mode: Device's priority in the CIST. In PVST mode: Device's priority in VLAN 1.
Max age(s)	Aging timer for BPDUs (in seconds, which is the same as the aging timer for VLAN 1 in PVST mode).
Forward delay(s)	Port state transition delay (in seconds, which is the same as the port state transition delay for VLAN 1 in PVST mode).
Hello time(s)	Interval for the root bridge to send BPDUs (in seconds, which is the same as the interval for VLAN 1 in PVST mode).
Max hops	Maximum hops in the MSTI.
TC Snooping	Status of TC Snooping: **Enabled** or **Disabled**.

Related commands

`reset stp`

display stp abnormal-port

Use **`display stp abnormal-port`** to display history about ports that are blocked by spanning tree protection features.

Syntax

`display stp abnormal-port`

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

In an MSTI or VLAN, this command can display a maximum of three history records for a port that is blocked by spanning tree protection features.

Examples

In MSTP mode, display history about ports that are blocked by spanning tree protection features.

```
---[GigabitEthernet1/0/1]---
    MST ID   BlockReason                    Time
    0        Root-Protected                 14:39:04 04/15/2016
    0        Root-Protected                 14:39:02 04/15/2016
    0        Root-Protected                 14:39:00 04/15/2016
```

In PVST mode, display history about ports that are blocked by spanning tree protection features.

```
---[GigabitEthernet1/0/1]---
    VLAN ID  BlockReason                    Time
    1        Root-Protected                 14:49:17 04/15/2016
    1        Root-Protected                 14:49:15 04/15/2016
    1        Root-Protected                 14:49:12 04/15/2016
```

Table 4 Command output

Field	Description
MST ID	MSTI of a blocked port.
VLAN ID	VLAN of a blocked port.
BlockReason	Reason that the port was blocked: • **Root-Protected**—Root guard feature. • **Loop-Protected**—Loop guard feature. • **Loopback-Protected**—Self-loop protection. A port in the MSTI receives a BPDU sent by itself. • **Disputed**—Dispute guard. A port receives a low-priority BPDU from a non-blocked designated port in forwarding or learning state. • **InconsistentPortType-Protected**—Inconsistent port type protection. • **InconsistentPvid-Protected**—Inconsistent PVID protection.
Time	Protection feature trigger time.

display stp bpdu-statistics

Use **display stp bpdu-statistics** to display the BPDU statistics for ports.

Syntax

display stp bpdu-statistics [**interface** *interface-type interface-number* [**instance** *instance-list*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

Usage guidelines

In MSTP mode, the command output is sorted by port name and by MSTI ID on each port.

- If you do not specify an MSTI or port, this command applies to all MSTIs on all ports.
- If you specify a port but not an MSTI, this command applies to all MSTIs on the port.
- If you specify both an MSTI ID and a port, this command applies to the specified MSTI on the port.

In STP, RSTP, or PVST mode, the command output is sorted by port name.

- If you do not specify a port, this command applies to all ports.
- If you specify a port, this command applies to the port.

Examples

In MSTP mode, display the BPDU statistics for all MSTIs on GigabitEthernet 1/0/1.

```
<Sysname> display stp bpdu-statistics interface gigabitethernet 1/0/1
 Port: GigabitEthernet1/0/1

 Instance-Independent:

 Type                        Count      Last Updated
 --------------------------- ---------- -----------------
 Invalid BPDUs               0
 Looped-back BPDUs           0
 Max-aged BPDUs              0
 TCN sent                    0
 TCN received                0
 TCA sent                    0
 TCA received                2          10:33:12 01/13/2011
```

```
 Config sent                 0
 Config received             0
 RST sent                    0
 RST received                0
 MST sent                    4          10:33:11 01/13/2011
 MST received                151        10:37:43 01/13/2011

 Instance 0:
 Type                        Count      Last Updated
 --------------------------- ---------- -----------------
 Timeout BPDUs               0
 Max-hoped BPDUs             0
 TC detected                 1          10:32:40 01/13/2011
 TC sent                     3          10:33:11 01/13/2011
 TC received                 0
```

In PVST mode, display the BPDU statistics for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] display stp bpdu-statistics interface gigabitethernet 1/0/1
 Port: GigabitEthernet1/0/1

 Type                        Count      Last Updated
 --------------------------- ---------- -----------------
 Invalid BPDUs               0
 Looped-back BPDUs           0
 Max-aged BPDUs              0
 TCN sent                    0
 TCN received                0
 TCA sent                    0
 TCA received                2           10:33:12 01/13/2010
 Config sent                 0
 Config received             0
 RST sent                    0
 RST received                0
 MST sent                    4           10:33:11 01/13/2010
 MST received                151         10:37:43 01/13/2010
 Timeout BPDUs               0
 Max-hoped BPDUs             0
 TC detected                 511         10:32:40 01/13/2010
 TC sent                     8844        10:33:11 01/13/2010
 TC received                 1426        10:33:32 01/13/2010
 PVID inconsistency BPDUs    0
```

Table 5 Command output

Field	Description
Port	Port name.
Instance-Independent	Statistics not related to a specific MSTI.

Field	Description
Type	Statistical item.
Looped-back BPDUs	Number of BPDUs sent and then received by the same port.
Max-aged BPDUs	Number of BPDUs whose max age was exceeded.
TCN sent	Number of sent TCN BPDUs.
TCN received	Number of received TCN BPDUs.
TCA sent	Number of sent TCA BPDUs.
TCA received	Number of received TCA BPDUs.
Config sent	Number of sent configuration BPDUs.
Config received	Number of received configuration BPDUs.
RST sent	Number of sent RSTP BPDUs.
RST received	Number of received RSTP BPDUs.
MST sent	Number of sent MSTP BPDUs.
MST received	Number of received MSTP BPDUs.
Instance	Statistics for a specific MSTI.
Timeout BPDUs	Number of expired BPDUs.
Max-hoped BPDUs	Number of BPDUs whose maximum hops were exceeded.
TC detected	Number of detected topology changes.
TC sent	Number of sent TC BPDUs.
TC received	Number of received TC BPDUs.
PVID inconsistency BPDUs	Number of received PVST BPDUs with a PVID inconsistent with the incoming port.

display stp down-port

Use **display stp down-port** to display information about ports that were shut down by spanning tree protection features.

Syntax

display stp down-port

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display information about ports that were shut down by spanning tree protection features.

```
<Sysname> display stp down-port
 Down Port                      Reason
 GigabitEthernet1/0/1           BPDU protection
```

Table 6 Command output

Field	Description
Down Port	Name of a port that was shut down by the spanning tree protection features.
Reason	Reason that the port was shut down: • **BPDU protection**—Indicates the BPDU guard feature. • **PVST BPDU protection**—Indicates the PVST BPDU guard feature.

display stp history

Use **display stp history** to display port role calculation history.

Syntax

display stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **history** [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices.

Usage guidelines

In STP or RSTP mode, the command output is sorted by port role calculation time.

In PVST mode, the command output is sorted by VLAN ID and by port role calculation time in each VLAN.

- If you do not specify a VLAN, this command applies to all VLANs.
- If you specify a VLAN list, this command applies to the specified VLANs.

In MSTP mode, the command output is sorted by MSTI ID and by port role calculation time in each MSTI.

- If you do not specify an MSTI, this command applies to all MSTIs.
- If you specify an MSTI list, this command applies to the specified MSTIs.

Examples

In MSTP mode, display the port role calculation history on the specified slot in MSTI 2.

```
<Sysname> display stp instance 2 history slot 1
```

```
 -------------- STP slot 1 history trace --------------
 ------------------  Instance 2   --------------------
Port GigabitEthernet1/0/1
   Role change         : ROOT->DESI (Aged)
   Time                : 2009/02/08 00:22:56
   Port priority       : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.1
   Designated priority : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.1
 Port GigabitEthernet1/0/2
   Role change         : ALTER->ROOT
   Time                : 2009/02/08 00:22:56
   Port priority       : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.2
                         128.153
   Designated priority : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.2
                         128.153
```

In PVST mode, display the port role calculation history on the specified slot in VLAN 2.

```
<Sysname> display stp vlan 2 history slot 1
 -------------- STP slot 1 history trace --------------
 ------------------  VLAN 2   --------------------

 Port GigabitEthernet1/0/1
   Role change         : ROOT->DESI (Aged)
   Time                : 2009/02/08 00:22:56
   Port priority       : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.1
   Designated priority : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.1
 Port GigabitEthernet1/0/2
   Role change         : ALTER->ROOT
   Time                : 2009/02/08 00:22:56
   Port priority       : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.2
   Designated priority : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.2
```

Table 7 Command output

Field	Description
Port	Port name.
Role change	Role change of the port (**Aged** means that the change was caused by expiration of the received configuration BPDU).
Time	Time of port role calculation.
Port priority	Current priority of the port: • For STP mode, RSTP mode, and ISTs (MSTI 0) in MSTP mode, port priority includes common root bridge ID, cost of the path to the common root bridge, regional root bridge ID, cost of the path to the regional root bridge, designated bridge ID, designated port ID, and ID of the port that receives messages from the designated port, which are separated with spaces. • For PVST mode and CSTs in MSTP mode, port priority includes regional root bridge ID, cost of the path to the regional root bridge, designated bridge ID, designated port ID, and ID of the port that receives messages from the designated port, which are separated with spaces.
Designated priority	Priority information reported by the current port as a designated port: • For STP mode, RSTP mode, and ISTs (MSTI 0) in MSTP mode, port priority includes common root bridge ID, cost of the path to the common root bridge,

Field	Description
	regional root bridge ID, cost of the path to the regional root bridge, device bridge ID, designated port ID, and current port ID, which are separated with spaces. • For PVST mode and CSTs in MSTP mode, port priority includes regional root bridge ID, cost of the path to the regional root bridge, device bridge ID, designated port ID, and current port ID, which are separated with spaces.

display stp region-configuration

Use **display stp region-configuration** to display effective MST region configuration.

Syntax

display stp region-configuration

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

In MSTP mode, display effective MST region configuration.

```
<Sysname> display stp region-configuration
 Oper Configuration
   Format selector      : 0
   Region name          : hello
   Revision level       : 0
   Configuration digest : 0x5f762d9a46311effb7a488a3267fca9f

   Instance   VLANs Mapped
   0          21 to 4094
   1          1 to 10
   2          11 to 20
```

Table 8 Command output

Field	Description
Format selector	Format selector that is defined by the spanning tree protocol. The default value is 0, and the selector cannot be configured.
Region name	MST region name.
Revision level	Revision level of the MST region. The default value is 0, and the level can be configured by using the **revision-level** command.
VLANs Mapped	VLANs mapped to the MSTI.

Related commands

instance

region-name

revision-level

vlan-mapping modulo

display stp root

Use **display stp root** to display the root bridge information of spanning trees.

Syntax

display stp root

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

In MSTP mode, display the root bridge information of all spanning trees.

```
<Sysname> display stp root
 MST ID  Root Bridge ID        ExtPathCost IntPathCost Root Port
 0       0.00e0-fc0e-6554      200200      0           GigabitEthernet1/0/1
```

In PVST mode, display the root bridge information of all spanning trees.

```
<Sysname> display stp root
 VLAN ID  Root Bridge ID        ExtPathCost IntPathCost Root Port
 1        0.00e0-fc0e-6554      200200      0           GigabitEthernet1/0/1
```

Table 9 Command output

Field	Description
ExtPathCost	External path cost. The path cost of a port is either automatically calculated by the device or manually configured by using the **stp cost** command.
IntPathCost	Internal path cost. The path cost of a port is either automatically calculated by the device or manually configured by using the **stp cost** command.
Root Port	Root port name (displayed only if a port of the device is the root port of the MSTI).

display stp tc

Use **display stp tc** to display the incoming and outgoing TC/TCN BPDU statistics for ports.

Syntax

display stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **tc** [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices.

Usage guidelines

In STP or RSTP mode, the command output is sorted by port name.

In PVST mode, the command output is sorted by VLAN ID and by port name in each VLAN.

- If you do not specify a VLAN, this command applies to all VLANs.
- If you specify a VLAN list, this command applies to the specified VLANs.

In MSTP mode, the command output is sorted by MSTI ID and by port name in each MSTI.

- If you do not specify an MSTI, this command applies to all MSTIs.
- If you specify an MSTI list, this command applies to the specified MSTIs.

Examples

In MSTP mode, display the incoming and outgoing TC/TCN BPDU statistics for all ports on slot 1 in MSTI 0.

```
<Sysname> display stp instance 0 tc slot 1
 -------------- STP slot 1 TC or TCN count -------------
 MST ID      Port                        Receive      Send
 0           GigabitEthernet1/0/1        6            4
 0           GigabitEthernet1/0/2        0            2
```

In PVST mode, display the incoming and outgoing TC/TCN BPDU statistics for all ports on slot 1 in VLAN 2.

```
<Sysname> display stp vlan 2 tc slot 1
 -------------- STP slot 1 TC or TCN count -------------
 VLAN ID     Port                        Receive      Send
 2           GigabitEthernet1/0/1        6            4
 2           GigabitEthernet1/0/2        0            2
```

Table 10 Command output

Field	Description
Port	Port name.
Receive	Number of TC/TCN BPDUs received on a port.
Send	Number of TC/TCN BPDUs sent by a port.

instance

Use **instance** to map a list of VLANs to an MSTI.

Use **undo instance** to remap the specified VLAN or all VLANs to the CIST (MSTI 0).

Syntax

instance *instance-id* **vlan** *vlan-id-list*

undo instance *instance-id* [**vlan** *vlan-id-list*]

Default

All VLANs are mapped to the CIST.

Views

MST region view

Predefined user roles

network-admin

Parameters

instance-id: Specifies an MSTI ID in the range of 0 to 4094. A value of 0 represents the CIST. The value range for the *instance-id* argument is 1 to 4094 for the **undo instance** command.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

CAUTION:

Use caution with global Digest Snooping in the following situations:

- When you modify the VLAN-to-instance mappings.
- When you restore the default MST region configuration.

If the local device has different VLAN-to-instance mappings than its neighboring devices, loops or traffic interruption will occur.

If you do not specify any VLANs in the **undo instance** command, all VLANs mapped to the specified MSTI are remapped to the CIST.

You cannot map a VLAN to different MSTIs. If you map a VLAN that has been mapped to an MSTI to a new MSTI, the old mapping is automatically deleted.

You can configure VLAN-to-instance mapping for up to 65 MSTIs.

After configuring this command, run the **active region-configuration** command to activate the VLAN-to-instance mapping.

Examples

Map VLAN 2 to MSTI 1.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] instance 1 vlan 2
```

Related commands

active region-configuration

check region-configuration

display stp region-configuration

region-name

Use **region-name** to configure the MST region name.

Use **undo region-name** to restore the default MST region name.

Syntax

region-name *name*

undo region-name

Default

The MST region name of the device is its MAC address.

Views

MST region view

Predefined user roles

network-admin

Parameters

name: Specifies the MST region name, a string of 1 to 32 characters.

Usage guidelines

The MST region name, the VLAN-to-instance mapping table, and the MSTP revision level of a device determine the device's MST region.

After configuring this command, execute the **active region-configuration** command to activate the configured MST region name.

Examples

Set the MST region name of the device to **hello**.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] region-name hello
```

Related commands

active region-configuration

check region-configuration

display stp region-configuration

instance

revision-level

vlan-mapping modulo

reset stp

Use **reset stp** to clear the spanning tree statistics.

Syntax

reset stp [**interface** *interface-list*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-list*: Specifies a space-separated list of up to 10 interface items. Each item specifies an interface or a range of interfaces in the form of *interface-type interface-number 1* [**to** *interface-type interface-number 2*]. The interface number for *interface-number 2* must be equal to or greater than the interface number for *interface-number 1*. If you do not specify this option, this command clears the spanning tree statistics on all ports.

Examples

Clear the spanning tree statistics on ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3.

```
<Sysname> reset stp interface gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

Related commands

display stp

revision-level

Use **revision-level** to configure the MSTP revision level.

Use **undo revision-level** to restore the default MSTP revision level.

Syntax

revision-level *level*

undo revision-level

Default

The MSTP revision level is 0.

Views

MST region view

Predefined user roles

network-admin

Parameters

level: Specifies an MSTP revision level in the range of 0 to 65535.

Usage guidelines

The MSTP revision level, the MST region name, and the VLAN-to-instance mapping table of a device determine the device's MST region.

After configuring this command, execute the **active region-configuration** command to activate the configured MST region level.

Examples

Set the MSTP revision level of the MST region to 5.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] revision-level 5
```

Related commands

active region-configuration

check region-configuration

display stp region-configuration

instance

region-name

vlan-mapping modulo

snmp-agent trap enable stp

Use **snmp-agent trap enable stp** to enable SNMP notifications for new-root election events or spanning tree topology changes.

Use **undo snmp-agent trap enable stp** to disable SNMP notifications for new-root election events or spanning tree topology changes.

Syntax

snmp-agent trap enable stp [**new-root** | **tc**]

undo snmp-agent trap enable stp [**new-root** | **tc**]

Default

SNMP notifications are disabled for new-root election events.

In MSTP mode, SNMP notifications are enabled in MSTI 0 and disabled in other MSTIs for spanning tree topology changes.

In PVST mode, SNMP notifications are disabled for spanning tree topology changes in all VLANs.

Views

System view

Predefined user roles

network-admin

Parameters

new-root: Enables the device to send notifications if the device is elected as a new root bridge. This keyword applies only to STP, MSTP, and RSTP modes.

tc: Enables the device to send notifications if the device receives TCN BPDUs. This keyword applies only to PVST mode.

Usage guidelines

If no keyword is specified, the **snmp-agent trap enable stp** command applies to SNMP notifications for different events as follows:

- In STP, MSTP, and RSTP modes, the command applies to SNMP notifications for new-root election events.
- In PVST mode, the command applies to SNMP notifications for spanning tree topology changes.

Examples

Enable SNMP notifications for new-root election events.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable stp new-root
```

stp bpdu-protection

Use **stp bpdu-protection** to enable BPDU guard globally.

Use **undo stp bpdu-protection** to disable BPDU guard globally.

Syntax

stp bpdu-protection

undo stp bpdu-protection

Default

BPDU guard is globally disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

With BPDU guard enabled, the device performs the following operations when edge ports receive configuration BPDUs:

- Shuts down these ports.
- Notifies the NMS that these ports have been shut down by the spanning tree protocol.

The device reactivates the ports that have been shut down when the port status detection timer expires. You can set this timer by using the **shutdown-interval** command. For more information about this command, see device management commands in *Fundamentals Command Reference*.

The global BPDU guard setting takes effect on all edge ports configured by using the **stp edged-port** command.

You can configure the BPDU guard feature globally or on a per-port basis. A port preferentially uses the port-specific BPDU guard setting. If the port-specific BPDU guard setting is not available, the port uses the global BPDU guard setting.

Examples

Enable BPDU guard globally.

```
<Sysname> system-view
[Sysname] stp bpdu-protection
```

Related commands

shutdown-interval (*Fundamentals Command Reference*)

stp edged-port

stp port bpdu-protection

stp bridge-diameter

Use **stp bridge-diameter** to set the network diameter. The switched network diameter refers to the maximum number of devices on the path for an edge device to reach another through the root bridge.

Use **undo stp bridge-diameter** to restore the default.

Syntax

stp [**vlan** *vlan-id-list*] **bridge-diameter** *diameter*

undo stp [**vlan** *vlan-id-list*] **bridge-diameter**

Default

The network diameter of the switched network is 7.

Views

System view

Predefined user roles

network-admin

Parameters

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094. If you set the STP, RSTP, or MSTP switched network diameter, do not specify this option.

diameter: Specifies the switched network diameter in the range of 2 to 7.

Usage guidelines

An appropriate setting of hello time, forward delay, and max age can speed up network convergence. The values of these timers are related to the network size, and you can set the timers by setting the network diameter. With the network diameter set to 7 (the default), the three timers are also set to their defaults.

In STP, RSTP, or MSTP mode, each MST region is considered as a device. The configured network diameter of the switched network takes effect only on the CIST (or the common root bridge).

In PVST mode, the configured network diameter takes effect only on the root bridges of the specified VLANs.

Examples

In MSTP mode, set the network diameter of the switched network to 5.

```
<Sysname> system-view
[Sysname] stp bridge-diameter 5
```

In PVST mode, set the network diameter of VLAN 2 in the switched network to 5.

```
<Sysname> system-view
[Sysname] stp vlan 2 bridge-diameter 5
```

Related commands

stp timer forward-delay

stp timer hello

stp timer max-age

stp compliance

Use **stp compliance** to configure the mode a port uses to recognize and send MSTP BPDUs.

Use **undo stp compliance** to restore the default.

Syntax

stp compliance { **auto** | **dot1s** | **legacy** }

undo stp compliance

Default

A port automatically recognizes the formats of received MSTP packets and determines the formats of MSTP packets to be sent based on the recognized formats.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

auto: Configures the port to recognize the MSTP BPDU format automatically and determine the format of MSTP BPDUs to send.

dot1s: Configures the port to receive and send only standard-format (802.1s-compliant) MSTP BPDUs.

legacy: Configures the port to receive and send only compatible-format MSTP BPDUs.

Usage guidelines

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Configure GigabitEthernet 1/0/1 to send only standard-format (802.1s) MSTP packets.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp compliance dot1s
```

stp config-digest-snooping

Use **stp config-digest-snooping** to enable Digest Snooping.

Use **undo stp config-digest-snooping** to disable Digest Snooping.

Syntax

stp config-digest-snooping

undo stp config-digest-snooping

Default

Digest Snooping is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

For Digest Snooping to take effect, you must enable Digest Snooping both globally and on associated ports. As a best practice, first enable Digest Snooping on ports connected to third-party vendor devices and then enable the feature globally. Digest Snooping takes effect on the ports simultaneously, which reduces impact on the network.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Enable Digest Snooping on GigabitEthernet 1/0/1 and then globally.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp config-digest-snooping
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] stp global config-digest-snooping
```

Related commands

display stp

stp global config-digest-snooping

stp cost

Use **stp cost** to set the path cost of a port.

Use **undo stp cost** to restore the default.

Syntax

stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **cost** *cost-value*

undo stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **cost**

Default

The device automatically calculates the path costs of ports in each spanning tree based on the corresponding standard.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for

vlan-id2 must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

cost-value: Specifies the path cost of the port, with an effective range that varies by path cost calculation standard that is used.

- When the IEEE 802.1d-1998 standard is selected for path cost calculation, the value range for the *cost* argument is 1 to 65535.
- When the IEEE 802.1t standard is selected for path cost calculation, the value range for the *cost* argument is 1 to 200000000.
- When the private standard is selected for path cost calculation, the value range for the *cost* argument is 1 to 200000.

Usage guidelines

Path cost is an important factor in spanning tree calculation. Setting different path costs for a port in MSTIs allows VLAN traffic flows to be forwarded along different physical links. This results in VLAN-based load balancing.

The path cost setting of a port can affect the role selection of the port. When the path cost of a port is changed, the system calculates the role of the port and initiates a state transition.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, is takes effect only after the port leaves the aggregation group.

If you do not specify an MSTI or VLAN, this command sets the path cost of a port in the MSTP CIST or in the STP or RSTP spanning tree.

Examples

In MSTP mode, set the path cost to 200 for GigabitEthernet 1/0/1 in MSTI 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp instance 2 cost 200
```

In PVST mode, set the path cost to 200 for GigabitEthernet 1/0/1 in VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp vlan 2 cost 200
```

Related commands

display stp

stp pathcost-standard

stp dispute-protection

Use **stp dispute-protection** to enable dispute guard.

Use **undo stp dispute-protection** to disable dispute guard.

Syntax

stp dispute-protection

undo stp dispute-protection

Default

Dispute guard is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Dispute guard blocks a port to prevent loops when a unidirectional link is detected on the port by the spanning tree feature.

In some VLAN networks, an uplink port on a downstream device is configured to deny packets from the PVID. As a result, the downstream device cannot receive BPDUs of the PVID from the upstream device. However, the upstream device can receive BPDUs from the downstream device. In this case, dispute guard blocks the receiving port on the upstream device, which causes traffic interruption.

To ensure service continuity and prevent the link from being blocked, you can disable dispute guard by using the **undo stp dispute-protection** command.

Examples

Disable dispute guard.

```
<Sysname> system-view
[Sysname] undo stp dispute-protection
```

stp edged-port

Use **stp edged-port** to configure a port as an edge port.

Use **undo stp edged-port** to restore the default.

Syntax

stp edged-port

undo stp edged-port

Default

All ports are non-edge ports.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

A port directly connecting to a user terminal rather than another device or a shared LAN segment can be configured as an edge port. In case the network topology changes, an edge port does not cause a temporary loop. You can enable the port to transit to the forwarding state rapidly by configuring it as an edge port. As a best practice, configure ports that directly connect to user terminals as edge ports.

Typically, configuration BPDUs from other devices cannot reach an edge port, because the edge port does not connect to any other device. When BPDU guard is disabled on a port configured as an edge port, the port acts as a non-edge port if it receives configuration BPDUs.

On a port, the loop guard feature and the edge port setting are mutually exclusive.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Configure GigabitEthernet 1/0/1 as an edge port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp edged-port
```

Related commands

stp bpdu-protection

stp loop-protection

stp port bpdu-protection

stp root-protection

stp enable

Use **stp enable** to enable the spanning tree feature.

Use **undo stp enable** to disable the spanning tree feature.

Syntax

stp enable

undo stp enable

Default

The spanning tree feature is enabled on all ports.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

When you enable the spanning tree feature, the device operates in STP, RSTP, PVST, or MSTP mode, depending on the spanning tree mode setting.

When you enable the spanning tree feature, the device dynamically maintains the spanning tree status of VLANs, based on received configuration BPDUs. When you disable the spanning tree feature, the device stops maintaining the spanning tree status.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

In MSTP mode, disable the spanning tree feature on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo stp enable
```

Related commands

stp global enable

stp mode

stp vlan enable

stp global config-digest-snooping

Use **stp global config-digest-snooping** to enable Digest Snooping globally.

Use **undo stp global config-digest-snooping** to disable Digest Snooping globally.

Syntax

stp global config-digest-snooping

undo stp global config-digest-snooping

Default

Digest Snooping is disabled globally.

Views

System view

Predefined user roles

network-admin

Usage guidelines

For Digest Snooping to take effect, you must enable Digest Snooping both globally and on associated ports. As a best practice, first enable Digest Snooping on ports connected to third-party vendor devices and then enable the feature globally. Digest Snooping takes effect on the ports simultaneously, which reduces impact on the network.

Examples

Enable Digest Snooping on GigabitEthernet 1/0/1 and then globally.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp config-digest-snooping
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] stp global config-digest-snooping
```

Related commands

display stp

stp config-digest-snooping

stp global enable

Use **stp global enable** to enable the spanning tree feature globally.

Use **undo stp global enable** to disable the spanning tree feature globally.

Syntax

stp global enable

undo stp global enable

Default

For the S5000V3-EI, S5000V5-EI, S5000E-X, S5000X-EI, and WAS6000 switch series, the spanning tree feature is globally disabled.

For other switch series:

- When the device starts up with initial settings, the spanning tree feature is globally disabled.
- When the device starts up with factory defaults, the spanning tree feature is globally enabled.

For more information about the initial settings and factory defaults, see *Fundamentals Configuration Guide*.

Views

System view

Predefined user roles

network-admin

Usage guidelines

When you enable the spanning tree feature, the device operates in STP, RSTP, PVST, or MSTP mode, depending on the spanning tree mode setting.

When the spanning tree feature is enabled, the device dynamically maintains the spanning tree status of VLANs based on received configuration BPDUs. When the spanning tree feature is disabled, the device stops maintaining the spanning tree status.

Examples

Enable the spanning tree feature globally.

```
<Sysname> system-view
[Sysname] stp global enable
```

Related commands

stp enable

stp mode

stp global mcheck

Use **stp global mcheck** to perform mCheck globally.

Syntax

stp global mcheck

Views

System view

Predefined user roles

network-admin

Usage guidelines

When a port on an MSTP, RSTP, or PVST device connects to an STP device and receives STP BPDUs, the port automatically transits to the STP mode. However, the port cannot automatically transit back to the original mode when the following conditions exist:

- The peer STP device is shut down or removed.
- The port cannot detect the change.

In this case, you can perform an mCheck operation to forcibly transit the port to operate in the original mode.

The device operates in STP, RSTP, PVST, or MSTP mode, depending on the spanning tree mode setting.

The **stp global mcheck** command takes effect only when the device operates in MSTP, RSTP, or PVST mode.

Examples

Perform mCheck globally.

```
<Sysname> system-view
[Sysname] stp global mcheck
```

Related commands

stp mcheck

stp mode

stp ignore-pvid-inconsistency

Use **stp ignore-pvid-inconsistency** to disable inconsistent PVID protection.

Use **undo stp ignore-pvid-inconsistency** to enable inconsistent PVID protection.

Syntax

stp ignore-pvid-inconsistency

undo stp ignore-pvid-inconsistency

Default

Inconsistent PVID protection is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only when the device is operating in PVST mode.

Disabling inconsistent PVID protection might cause spanning tree calculation errors. To avoid such errors, make sure the following requirements are met:

- Make sure the VLANs on one device do not use the same ID as the PVID of its peer port (except the default VLAN) on another device.
- If the local port or its peer is a hybrid port, do not configure the local and peer ports as untagged members of the same VLAN.
- Disable inconsistent PVID protection on both the local device and the peer device.

Examples

In PVST mode, disable the inconsistent PVID protection feature.

```
<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] stp ignore-pvid-inconsistency
```

stp log enable tc

Use **stp log enable tc** to enable the device to log events of detecting or receiving TC BPDUs.

Use **undo stp log enable tc** to restore the default.

Syntax

stp log enable tc

undo stp log enable tc

Default

In PVST mode, the device does not generate logs when it detects or receives TC BPDUs.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command applies only to PVST mode.

Examples

In PVST mode, enable the device to log events of detecting or receiving TC BPDUs.

```
<Sysname> system-view
[Sysname] stp log enable tc
```

stp loop-protection

Use **stp loop-protection** to enable loop guard on a port.

Use **undo stp loop-protection** to disable loop guard on a port.

Syntax

stp loop-protection

undo stp loop-protection

Default

Loop guard is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

On a port, the loop guard feature is mutually exclusive with the root guard feature or the edge port setting.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Enable loop guard on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp loop-protection
```

Related commands

stp edged-port

stp root-protection

stp max-hops

Use **stp max-hops** to set the maximum number of hops for an MST region.

Use **undo stp max-hops** to restore the default.

Syntax

stp max-hops *hops*

undo stp max-hops

Default

The maximum number of hops for an MST region is 20.

Views

System view

Predefined user roles

network-admin

Parameters

hops: Specifies the maximum hops in the range of 1 to 40.

Examples

Set the maximum hops of the MST region to 35.

```
<Sysname> system-view
[Sysname] stp max-hops 35
```

Related commands

display stp

stp mcheck

Use **stp mcheck** to perform mCheck on a port.

Syntax

stp mcheck

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

When a port on an MSTP, RSTP, or PVST device connects to an STP device and receives STP BPDUs, the port automatically transits to the STP mode. However, the port cannot automatically transit back to the original mode when the following conditions exist:

- The peer STP device is shut down or removed.
- The port cannot detect the change.

In this case, you can perform an mCheck operation to forcibly transit the port to operation in the original mode.

For example, Device A, Device B, and Device C are connected in sequence. Device A runs STP, Device B does not run any spanning tree protocol, and Device C runs RSTP, MSTP, or PVST. When Device C receives an STP BPDU transparently transmitted by Device B, the receiving port transits to the STP mode. If you configure Device B to run RSTP, MSTP, or PVST with Device C, perform mCheck operations on the ports that connect Device B and Device C.

The device operates in STP, RSTP, PVST, or MSTP mode, depending on the spanning tree mode setting.

The **stp mcheck** command takes effect only when the device operates in MSTP, RSTP, or PVST mode.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Perform mCheck on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp mcheck
```

Related commands

stp global mcheck

stp mode

stp mode

Use **stp mode** to configure the spanning tree operating mode.

Use **undo stp mode** to restore the default.

Syntax

stp mode { **mstp** | **pvst** | **rstp** | **stp** }

undo stp mode

Default

A spanning tree device operates in MSTP mode.

Views

System view

Predefined user roles

network-admin

Parameters

mstp: Configures the spanning tree device to operate in MSTP mode.

pvst: Configures the spanning tree device to operate in PVST mode.

rstp: Configures the spanning tree device to operate in RSTP mode.

stp: Configures the spanning tree device to operate in STP mode.

Usage guidelines

The MSTP mode is compatible with the RSTP mode, and the RSTP mode is compatible with the STP mode.

The PVST mode's compatibility with other modes is as follows:

- **Access port**—The PVST mode is compatible with other modes in any VLAN.
- **Trunk or hybrid port**—The PVST mode is compatible with other modes only in the default VLAN.

Examples

Configure the spanning tree device to operate in STP mode.

```
<Sysname> system-view
[Sysname] stp mode stp
```

Related commands

stp enable

stp global enable

stp global mcheck

stp mcheck

stp vlan enable

stp no-agreement-check

Use **stp no-agreement-check** to enable No Agreement Check on a port.

Use **undo stp no-agreement-check** to disable No Agreement Check on a port.

Syntax

stp no-agreement-check

undo stp no-agreement-check

Default

No Agreement Check is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only after you enable it on the root port.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Enable No Agreement Check on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp no-agreement-check
```

stp pathcost-standard

Use **stp pathcost-standard** to specify a standard for the device to use when calculating the default path costs for ports.

Use **undo stp pathcost-standard** to restore the default.

Syntax

stp pathcost-standard { **dot1d-1998** | **dot1t** | **legacy** }

undo stp pathcost-standard

Default

The default standard used by the device is **legacy**.

Views

System view

Predefined user roles

network-admin

Parameters

dot1d-1998: Configures the device to calculate the default path cost for ports based on IEEE 802.1d-1998.

dot1t: Configures the device to calculate the default path cost for ports based on IEEE 802.1t.

legacy: Configures the device to calculate the default path cost for ports based on a private standard.

Usage guidelines

If you change the standard that the device uses in calculating the default path costs, you restore the path costs to the default.

Examples

Configure the device to calculate the default path cost for ports based on IEEE 802.1d-1998.

```
<Sysname> system-view
[Sysname] stp pathcost-standard dot1d-1998
```

Related commands

display stp

stp cost

stp point-to-point

Use **stp point-to-point** to configure the link type of a port.

Use **undo stp point-to-point** to restore the default.

Syntax

stp point-to-point { **auto** | **force-false** | **force-true** }

undo stp point-to-point

Default

The default setting is **auto,** and the spanning tree device automatically detects whether a port connects to a point-to-point link.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

auto: Specifies automatic detection of the link type.

force-false: Specifies the non-point-to-point link type.

force-true: Specifies the point-to-point link type.

Usage guidelines

When connecting to a non-point-to-point link, a port is incapable of rapid state transition.

You can configure the link type as point-to-point for a Layer 2 aggregate interface or a port that operates in full duplex mode. As a best practice, use the default setting to let the device automatically detect the port link type.

In MSTP or PVST mode, the **stp point-to-point force-false** or **stp point-to-point force-true** command configured on a port takes effect on all MSTIs or VLANs.

Before you set the link type of a port to point-to-point, make sure the port is connected to a point-to-point link. Otherwise, a temporary loop might occur.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Configure the link type of GigabitEthernet 1/0/1 as point-to-point.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp point-to-point force-true
```

Related commands

display stp

stp port bpdu-protection

Use **stp port bpdu-protection** to configure BPDU guard on an interface.

Use **undo stp port bpdu-protection** to restore the default.

Syntax

stp port bpdu-protection { **enable** | **disable** }

undo stp port bpdu-protection

Default

BPDU guard is not configured on a per-edge port basis. The status of BPDU guard on an interface is the same as the global BPDU guard status.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

enable: Enables BPDU guard.

disable: Disables BPDU guard.

Usage guidelines

With BPDU guard enabled, the device performs the following operations when an edge port receives configuration BPDUs:

- Shuts down the port.
- Notifies the NMS that the port has been shut down by the spanning tree protocol.

The device reactivates the port that has been shut down when the port status detection timer expires. You can set this timer by using the **shutdown-interval** command. For more information about this command, see device management commands in *Fundamentals Command Reference*.

You can configure the BPDU guard feature globally or on a per-port basis. A port preferentially uses the port-specific BPDU guard setting. If the port-specific BPDU guard setting is not available, the port uses the global BPDU guard setting.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Enable BPDU guard on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp port bpdu-protection enable
```

Related commands

shutdown-interval (*Fundamentals Command Reference*)

stp bpdu-protection

stp edged-port

stp port priority

Use **stp port priority** to set the priority of a port. The port priority affects the role of a port in a spanning tree.

Use **undo stp port priority** to restore the default.

Syntax

stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **port priority** *priority*

undo stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **port priority**

Default

The port priority is 128.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

priority: Specifies the port priority in the range of 0 to 240 in increments of 16 (as in 0, 16, 32).

Usage guidelines

The smaller the value, the higher the port priority. If all ports on your device use the same priority value, the port priority depends on the port index. The smaller the index, the higher the priority.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

If you do not specify an MSTI or VLAN, this command configures the priority of the ports in the MSTP CIST or in the STP or RSTP spanning tree.

Examples

In MSTP mode, set the port priority of GigabitEthernet 1/0/1 to 16 in MSTI 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp instance 2 port priority 16
```

In PVST mode, set the port priority of GigabitEthernet 1/0/1 to 16 in VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp vlan 2 port priority 16
```

Related commands

display stp

stp port shutdown permanent

Use **stp port shutdown permanent** to disable the device from reactivating edge ports shut down by BPDU guard.

Use **undo stp port shutdown permanent** to restore the default.

Syntax

stp port shutdown permanent

undo stp port shutdown permanent

Default

The device reactivates an edge port shut down by BPDU guard after the port status detection timer expires.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only on edge ports shut down by BPDU guard after this command is configured. The device does not bring up the shutdown ports if you execute the **undo stp port shutdown permanent** command. To bring up these ports, you must use the **undo shutdown** command.

For more information about the port status detection timer, see device management configuration in *Fundamentals Configuration Guide*.

Examples

Disable the device from reactivating edge ports shut down by BPDU guard.

```
<Sysname> system-view
[Sysname] stp port shutdown permanent
```

stp port-log

Use **stp port-log** to enable outputting port state transition information.

Use **undo stp port-log** to disable outputting port state transition information.

Syntax

stp port-log { **all** | **instance** *instance-list* | **vlan** *vlan-id-list* }

undo stp port-log { **all** | **instance** *instance-list* | **vlan** *vlan-id-list* }

Default

The default differs depending on the software version, as shown below:

Hardware platform	Versions	Default setting
S5000V3-EI, S5000V5-EI, S5000E-X, S5000X-EI, WAS6000	All versions	Outputting port state transition information is disabled.
Other switch series	Versions earlier than Release 6350	Outputting port state transition information is disabled.
	Release 6350 and later	• If the device starts up with the initial configuration, outputting port state transition information is disabled. • If the device starts up with the factory defaults, outputting port state transition information is enabled.

For more information about initial configuration and factory defaults, see configuration file management in *Fundamentals Configuration Guide*.

Views

System view

Predefined user roles

network-admin

Parameters

all: Specifies all MSTIs or VLANs.

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

Examples

In MSTP mode, enable outputting port state transition information for MSTI 2.

```
<Sysname> system-view
[Sysname] stp port-log instance 2
%Aug 16 00:49:41:856 2011 Sysname STP/3/STP_DISCARDING: Instance 2's port
GigabitEthernet1/0/1 has been set to discarding state.
%Aug 16 00:49:41:856 2011 Sysname STP/3/STP_FORWARDING: Instance 2's port
GigabitEthernet1/0/2 has been set to forwarding state.
```

The output shows that GigabitEthernet 1/0/1 in MSTI 2 transited to the discarding state and GigabitEthernet 1/0/2 in MSTI 2 transited to the forwarding state.

In PVST mode, enable outputting port state transition information for VLAN 1 through VLAN 4094.

```
<Sysname> system-view
[Sysname] stp port-log vlan 1 to 4094
%Aug 16 00:49:41:856 2006 Sysname STP/3/STP_DISCARDING: VLAN 2's GigabitEthernet1/0/1 has been set to discarding state.
%Aug 16 00:49:41:856 2006 Sysname STP/3/STP_FORWARDING: VLAN 2's GigabitEthernet1/0/2 has been set to forwarding state.
```

The output shows that GigabitEthernet 1/0/1 in VLAN 2 transited to the discarding state and GigabitEthernet 1/0/2 in VLAN 2 transited to the forwarding state.

stp priority

Use **stp priority** to set the priority of the device.

Use **undo stp priority** to restore the default.

Syntax

stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **priority** *priority*

undo stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **priority**

Default

The device priority is 32768.

Views

System view

Predefined user roles

network-admin

Parameters

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

priority: Specifies the device priority in the range of 0 to 61440 in increments of 4096 (as in 0, 4096, 8192). You can set up to 16 priority values on the device. The smaller the value, the higher the device priority.

Usage guidelines

If you do not specify an MSTI or VLAN, this command configures the priority of the device in the MSTP CIST or in the STP or RSTP spanning tree.

Examples

In MSTP mode, set the device priority to 4096 in MSTI 1.

```
<Sysname> system-view
[Sysname] stp instance 1 priority 4096
```

In PVST mode, set the device priority to 4096 in VLAN 1.

```
<Sysname> system-view
```

```
[Sysname] stp vlan 1 priority 4096
```

stp pvst-bpdu-protection

Use **stp pvst-bpdu-protection** to enable PVST BPDU guard.

Use **undo stp pvst-bpdu-protection** to disable PVST BPDU guard.

Syntax

stp pvst-bpdu-protection

undo stp pvst-bpdu-protection

Default

PVST BPDU guard is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

PVST BPDU guard enables an MSTP-enabled device to shut down a port if the port receives PVST BPDUs. The shutdown port is brought up after a detection timer expires. To set the detection timer, use the **shutdown-interval** command.

Examples

In MSTP mode, enable PVST BPDU guard.

```
<Sysname> system-view
[Sysname] stp pvst-bpdu-protection
```

Related commands

shutdown-interval (For more information, see *Fundamentals Command Reference*.)

stp region-configuration

Use **stp region-configuration** to enter MST region view.

Use **undo stp region-configuration** to restore the default MST region configurations.

Syntax

stp region-configuration

undo stp region-configuration

Default

The default settings for an MST region are as follows:

- The MST region name of the device is its MAC address.
- All VLANs are mapped to the CIST.
- The MSTP revision level is 0.

Views

System view

Predefined user roles

network-admin

Usage guidelines

After you enter MST region view, you can configure MST region parameters, including the region name, VLAN-to-instance mappings, and revision level.

Examples

Enter MST region view.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region]
```

stp role-restriction

Use **stp role-restriction** to enable port role restriction.

Use **undo stp role-restriction** to disable port role restriction.

Syntax

stp role-restriction

undo stp role-restriction

Default

Port role restriction is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

When port role restriction is enabled on a port, the port cannot become a root port.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Enable port role restriction on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp role-restriction
```

stp root primary

Use **stp root primary** to configure the device as the root bridge.

Use **undo stp root** to restore the default.

Syntax

stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **root primary**

undo stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **root**

Default

The device is not a root bridge.

Views

System view

Predefined user roles

network-admin

Parameters

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

Once you specify the device as the root bridge, you cannot change the priority of the device.

If you do not specify an MSTI or VLAN, this command configures the device as the root bridge of the MSTP CIST or of the STP or RSTP spanning tree.

Examples

In MSTP mode, specify the device as the root bridge of MSTI 1.

```
<Sysname> system-view
[Sysname] stp instance 1 root primary
```

In PVST mode, specify the device as the root bridge of VLAN 1.

```
<Sysname> system-view
[Sysname] stp vlan 1 root primary
```

Related commands

stp priority

stp root secondary

stp root secondary

Use **stp root secondary** to configure the device as a secondary root bridge.

Use **undo stp root** to restore the default.

Syntax

stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **root secondary**

undo stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **root**

Default

The device is not a secondary root bridge.

Views

System view

Predefined user roles

network-admin

Parameters

instance *instance-list*: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* [**to** *instance-id2*]. The value for *instance-id2* must be equal to or greater than the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094, and the value 0 represents the CIST.

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

Once you specify the device as a secondary root bridge, you cannot change the priority of the device.

If you do not specify an MSTI or VLAN, this command configures a secondary root bridge for the MSTP CIST or the STP or RSTP spanning tree.

Examples

In MSTP mode, specify the device as a secondary root bridge in MSTI 1.

```
<Sysname> system-view
[Sysname] stp instance 1 root secondary
```

In PVST mode, specify the device as a secondary root bridge in VLAN 1.

```
<Sysname> system-view
[Sysname] stp vlan 1 root secondary
```

Related commands

stp priority

stp root primary

stp root-protection

Use **stp root-protection** to enable root guard on a port.

Use **undo stp root-protection** to disable root guard on a port.

Syntax

stp root-protection

undo stp root-protection

Default

Root guard is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

On a port, the loop guard feature and the root guard feature are mutually exclusive.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Enable root guard on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp root-protection
```

Related commands

stp edged-port

stp loop-protection

stp tc-protection

Use **stp tc-protection** to enable TC-BPDU attack guard for the device.

Use **undo stp tc-protection** to disable TC-BPDU attack guard for the device.

Syntax

stp tc-protection

undo stp tc-protection

Default

TC-BPDU attack guard is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

With TC-BPDU guard, you can set the maximum number of immediate forwarding address entry flushes that the device can perform every 10 seconds. For TC-BPDUs received that exceed the limit, the device performs a forwarding address entry flush when the interval elapses. This prevents frequent flushing of forwarding address entries.

Examples

Disable TC-BPDU attack guard for the device.

```
<Sysname> system-view
[Sysname] undo stp tc-protection
```

Related commands

stp tc-protection threshold

stp tc-protection threshold

Use **stp tc-protection threshold** to set the maximum number of forwarding address entry flushes that the device can perform every 10 seconds.

Use **undo stp tc-protection threshold** to restore the default.

Syntax

stp tc-protection threshold *number*

undo stp tc-protection threshold

Default

By default, the device can perform a maximum of 6 forwarding address entry flushes every 10 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

number: Specifies the maximum number of immediate forwarding address entry flushes that the device can perform every 10 seconds. The value is in the range of 1 to 255.

Examples

Configure the device to perform up to 10 forwarding address entry flushes every 10 seconds.

```
<Sysname> system-view
[Sysname] stp tc-protection threshold 10
```

Related commands

stp tc-protection

stp tc-restriction

Use **stp tc-restriction** to enable TC-BPDU transmission restriction.

Use **undo stp tc-restriction** to disable TC-BPDU transmission restriction.

Syntax

stp tc-restriction

undo stp tc-restriction

Default

TC-BPDU transmission restriction is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

When TC-BPDU transmission restriction is enabled on a port, the port does not send TC-BPDUs to other ports. It also does not delete MAC address entries.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Enable TC-BPDU transmission restriction on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp tc-restriction
```

stp tc-snooping

Use **stp tc-snooping** to enable TC Snooping.

Use **undo stp tc-snooping** to disable TC Snooping.

Syntax

stp tc-snooping

undo stp tc-snooping

Default

TC Snooping is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

TC Snooping and the spanning tree feature are mutually exclusive. You must globally disable the spanning tree feature before enabling TC Snooping.

Examples

Globally disable the spanning tree feature and enable TC Snooping.

```
<Sysname> system-view
[Sysname] undo stp global enable
[Sysname] stp tc-snooping
```

Related commands

stp global enable

stp timer forward-delay

Use **stp timer forward-delay** to set the forward delay timer.

Use **undo stp timer forward-delay** to restore the default.

Syntax

stp [**vlan** *vlan-id-list*] **timer forward-delay** *time*

undo stp [**vlan** *vlan-id-list*] **timer forward-delay**

Default

The forward delay timer is 1500 centiseconds.

Views

System view

Predefined user roles

network-admin

Parameters

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094. If you set the STP, RSTP, or MSTP forward delay, do not specify this option.

time: Specifies the forward delay in centiseconds, in the range of 400 to 3000 in increments of 100 (as in 400, 500, 600).

Usage guidelines

The forward delay timer determines the time interval of state transition. To prevent temporary loops, a spanning tree port goes through the learning (intermediate) state before it transits from the discarding state to the forwarding state. To stay synchronized with the remote device, the port has a wait period that is determined by the forward delay timer between transition states.

As a best practice, do not set the forward delay with this command. Instead, you can specify the network diameter of the switched network by using the **stp bridge-diameter** command. This command makes the spanning tree protocols automatically calculate the optimal settings for the forward delay timer. If the network diameter uses the default value, the forward delay timer also uses the default value.

Examples

In MSTP mode, set the forward delay timer to 2000 centiseconds.

```
<Sysname> system-view
[Sysname] stp timer forward-delay 2000
```

In PVST mode, set the forward delay timer for VLAN 2 to 2000 centiseconds.

```
<Sysname> system-view
[Sysname] stp vlan 2 timer forward-delay 2000
```

Related commands

stp bridge-diameter

stp timer hello

stp timer max-age

stp timer hello

Use **stp timer hello** to set the hello time.

Use **undo stp timer hello** to restore the default.

Syntax

stp [**vlan** *vlan-id-list*] **timer hello** *time*

undo stp [**vlan** *vlan-id-list*] **timer hello**

Default

The hello time is 200 centiseconds.

Views

System view

Predefined user roles

network-admin

Parameters

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094. If you set the STP, RSTP, or MSTP hello time, do not specify this option.

time: Specifies the hello time in centiseconds, in the range of 100 to 1000 in increments of 100 (as in 100, 200, 300).

Usage guidelines

Hello time is the interval at which spanning tree devices send configuration BPDUs to maintain the spanning tree. If a device fails to receive configuration BPDUs within the set period of time, a new spanning tree calculation process is triggered.

As a best practice, do not set the hello time with this command. Instead, you can specify the network diameter of the switched network by using the **stp bridge-diameter** command. This command makes the spanning tree protocols automatically calculate the optimal settings for the hello timer. If the network diameter uses the default value, the hello timer also uses the default value.

Examples

In MSTP mode, set the hello time to 400 centiseconds.

```
<Sysname> system-view
[Sysname] stp timer hello 400
```

In PVST mode, set the hello time for VLAN 2 to 400 centiseconds.

```
<Sysname> system-view
[Sysname] stp vlan 2 timer hello 400
```

Related commands

stp bridge-diameter

stp timer forward-delay

stp timer max-age

stp timer max-age

Use **stp timer max-age** to set the max age timer.

Use **undo stp timer max-age** to restore the default.

Syntax

stp [**vlan** *vlan-id-list*] **timer max-age** *time*

undo stp [**vlan** *vlan-id-list*] **timer max-age**

Default

The max age is 2000 centiseconds.

Views

System view

Predefined user roles

network-admin

Parameters

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094. If you set the STP, RSTP, or MSTP max age, do not specify this option.

time: Specifies the max age in centiseconds, in the range of 600 to 4000 in increments of 100 (as in 600, 700, 800).

Usage guidelines

In the CIST of an MSTP network, the device determines whether a configuration BPDU received on a port has expired based on the max age timer. If the configuration BPDU has expired, a new spanning tree calculation process starts. The max age timer takes effect only on the CIST (or MSTI 0).

As a best practice, do not set the max age timer with this command. Instead, you can specify the network diameter of the switched network by using the **stp bridge-diameter** command. This command makes the spanning tree protocols automatically calculate the optimal settings for the max age timer. If the network diameter uses the default value, the max age timer also uses the default value.

Examples

In MSTP mode, set the max age timer to 1000 centiseconds.

```
<Sysname> system-view
[Sysname] stp timer max-age 1000
```

In PVST mode, set the max age timer for VLAN 2 to 1000 centiseconds.

```
<Sysname> system-view
[Sysname] stp vlan 2 timer max-age 1000
```

Related commands

stp bridge-diameter

stp timer forward-delay

stp timer hello

stp timer-factor

Use **stp timer-factor** to configure the timeout period by setting the timeout factor.

Timeout period = timeout factor × 3 × hello time.

Use **undo stp timer-factor** to restore the default.

Syntax

stp timer-factor *factor*

undo stp timer-factor

Default

The timeout factor of the device is set to 3.

Views

System view

Predefined user roles

network-admin

Parameters

factor: Specifies the timeout factor in the range of 1 to 20.

Usage guidelines

In a stable network, each non-root-bridge forwards configuration BPDUs to surrounding devices at the interval of hello time to determine whether any link fails. If a device does not receive a BPDU from the upstream device within nine times of the hello time, it assumes that the upstream device has failed. Then it will start a new spanning tree calculation process.

As a best practice, set the timeout factor to 5, 6, or 7 in the following situations:

- To prevent undesired spanning tree calculations. An upstream device might be too busy to forward configuration BPDUs in time, for example, many Layer 2 interfaces are configured on the upstream device. In this case, the downstream device fails to receive a BPDU within the timeout period and then starts an undesired spanning tree calculation.
- To save network resources on a stable network.

Examples

Set the timeout factor of the device to 7.

```
<Sysname> system-view
[Sysname] stp timer-factor 7
```

Related commands

stp timer hello

stp transmit-limit

Use **stp transmit-limit** to set the BPDU transmission rate of a port.

Use **undo stp transmit-limit** to restore the default.

Syntax

stp transmit-limit *limit*

undo stp transmit-limit

Default

The BPDU transmission rate of all ports is 10.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

limit: Specifies the BPDU transmission rate in the range of 1 to 255.

Usage guidelines

The maximum number of BPDUs a port can send within each hello time equals the BPDU transmission rate plus the hello timer value.

A larger BPDU transmission rate value requires more system resources. An appropriate BPDU transmission rate setting can prevent spanning tree protocols from using excessive bandwidth resources during network topology changes. As a best practice, use the default value.

If this command is configured in Layer 2 Ethernet interface view, it takes effect only on that interface.

If this command is configured in Layer 2 aggregate interface view, it takes effect only on the aggregate interface.

If this command is configured on a member port in an aggregation group, it takes effect only after the port leaves the aggregation group.

Examples

Set the BPDU transmission rate of GigabitEthernet 1/0/1 to 5.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp transmit-limit 5
```

stp vlan enable

Use **stp vlan enable** to enable the spanning tree feature for VLANs.

Use **undo stp enable** to disable the spanning tree feature for VLANs.

Syntax

stp vlan *vlan-id-list* **enable**

undo stp vlan *vlan-id-list* **enable**

Default

The spanning tree feature is enabled in VLANs.

Views

System view

Predefined user roles

network-admin

Parameters

vlan *vlan-id-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

When you enable the spanning tree feature, the device operates in STP, RSTP, PVST, or MSTP mode, depending on the spanning tree mode setting.

When you enable the spanning tree feature, the device dynamically maintains the spanning tree status of VLANs, based on received configuration BPDUs. When you disable the spanning tree feature, the device stops maintaining the spanning tree status.

Examples

In PVST mode, globally enable the spanning tree feature and then enable the spanning tree feature for VLAN 2.

```
<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] stp global enable
[Sysname] stp vlan 2 enable
```

Related commands

stp enable

stp global enable

stp mode

vlan-mapping modulo

Use **vlan-mapping modulo** to map VLANs in an MST region to MSTIs according to the specified modulo value and quickly create a VLAN-to-instance mapping table.

Syntax

vlan-mapping modulo *modulo*

Default

All VLANs are mapped to the CIST (MSTI 0).

Views

MST region view

Predefined user roles

network-admin

Parameters

modulo: Specifies the modulo value. The value range for this argument is 1 to 64.

Usage guidelines

You cannot map a VLAN to different MSTIs. If you map a VLAN that has been mapped to an MSTI to a new MSTI, the old mapping is automatically deleted.

This command maps each VLAN to the MSTI with ID (VLAN ID – 1) % *modulo* + 1. (VLAN ID – 1) % *modulo* is the modulo operation for (VLAN ID – 1). If the modulo value is 15, then VLAN 1 is mapped to MSTI 1, VLAN 2 to MSTI 2, …, VLAN 15 to MSTI 15, VLAN 16 to MSTI 16, and so on.

Examples

Map VLANs to MSTIs as per modulo 8.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] vlan-mapping modulo 8
```

Related commands

active region-configuration

check region-configuration

display stp region-configuration

region-name

revision-level

Contents

Loop detection commands

display loopback-detection

Use **display loopback-detection** to display the loop detection configuration and status.

Syntax

display loopback-detection

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

In the command output, a port shut down by loop detection stays in looped state until it comes up.

Example

Display the loop detection configuration and status.

```
<Sysname> display loopback-detection
Loop detection is enabled.
Loop detection interval is 30 second(s).
Loop is detected on following interfaces:
 Interface                     Action mode     VLANs
 GigabitEthernet1/0/3          None            10
```

Table 1 Command output

Field	Description

Action mode	Loop protection action:
	• **Block**—When a loop is detected on a port, the device performs the following operations:
	  ○ Generates a log.
	  ○ Disables the port from learning MAC addresses.
	  ○ Blocks the port.
	• **None**—When a loop is detected on a port, the device generates a log but performs no action on the port.
	• **No-learning**—When a loop is detected on a port, the device generates a log and disables the port from learning MAC addresses.
	• **Shutdown**—When a loop is detected on a port, the device performs the following operations:
	  ○ Generates a log.
	  ○ Shuts down the port to disable the port from receiving or sending frames. The device automatically sets the port to the forwarding state after a time interval. Set the time interval by using the **shutdown-interval** command (see *Fundamentals Command Reference*).

VLANs	VLANs to which the interface belongs and where loops are detected.

loopback-detection action

Use **loopback-detection action** to set the loop protection action on a per-port basis.

Use **undo loopback-detection action** to restore the default.

Syntax

In Layer 2 Ethernet interface view:

loopback-detection action { **block** | **no-learning** | **shutdown** }

undo loopback-detection action

In Layer 2 aggregate interface view:

loopback-detection action shutdown

undo loopback-detection action

Default

When the device detects a loop on a port, it generates a log but performs no action on the port.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

block: Enables the block mode. If a loop is detected, the device performs the following operations:

- Generates a log.
- Disables MAC address learning.
- Blocks the port.

Layer 2 aggregate interfaces do not support this keyword.

no-learning: Enables the no-learning mode. If a loop is detected, the device generates a log and disables MAC address learning on the port. Layer 2 aggregate interfaces do not support this keyword.

shutdown: Enables the shutdown mode. If a loop is detected, the device generates a log and shuts down the port. The device automatically sets the port to the forwarding state after the time interval set by using the **shutdown-interval** command (see *Fundamentals Command Reference*).

Usage guidelines

To set the loop protection action globally, use the **loopback-detection global action** command.

The global action applies to all ports. The per-port action applies to the individual ports. The per-port action takes precedence over the global action.

Example

Set the loop protection action to **shutdown** on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[System-GigabitEthernet1/0/1] loopback-detection action shutdown
```

Related commands

display loopback-detection

loopback-detection global action

loopback-detection enable

Use **loopback-detection enable** to enable loop detection on a per-port basis.

Use **undo loopback-detection enable** to disable loop detection on a port.

Syntax

loopback-detection enable vlan { *vlan-id-list* | **all** }

undo loopback-detection enable vlan { *vlan-id-list* | **all** }

Default

Loop detection is disabled on ports.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN ID or a range of VLAN IDs in the form of *vlan-id1* to *vlan-id2*. The value range for VLAN IDs is 1 to 4094. The ID for *vlan-id2* must be no less than the ID for *vlan-id1*.

all: Specifies all existing VLANs.

Usage guidelines

You can enable loop detection globally or on a per-port basis. When a port receives a detection frame in any VLAN, the loop protection action is triggered on that port, regardless of whether loop detection is enabled on it.

Example

Enable loop detection on GigabitEthernet 1/0/1 for VLAN 10 through VLAN 20.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[System-GigabitEthernet1/0/1] loopback-detection enable vlan 10 to 20
```

Related commands

display loopback-detection

loopback-detection global enable

loopback-detection global action

Use **loopback-detection global action** to set the global loop protection action.

Use **undo loopback-detection global action** to restore the default.

Syntax

loopback-detection global action shutdown

undo loopback-detection global action

Default

When the device detects a loop on a port, it generates a log but performs no action on the port.

Views

System view

Predefined user roles

network-admin

Parameters

shutdown: Enables the shutdown mode. If a loop is detected, the device generates a log and shuts down the port. The device automatically sets the port to the forwarding state after you set the time interval by using the **shutdown-interval** command (see *Fundamentals Command Reference*).

Usage guidelines

To set the loop protection action on a per-port basis, use the **loopback-detection action** command in interface view.

The global action applies to all ports. The per-port action applies to the individual ports. The per-port action takes precedence over the global action.

Example

Set the global loop protection action to **shutdown**.

```
<Sysname> system-view
[System] loopback-detection global action shutdown
```

Related commands

display loopback-detection

loopback-detection action

loopback-detection global enable

Use **loopback-detection global enable** to enable loop detection globally.

Use **undo loopback-detection global enable** to disable loop detection globally.

Syntax

loopback-detection global enable vlan { *vlan-id-list* | **all** }

undo loopback-detection global enable vlan { *vlan-id-list* | **all** }

Default

Loop detection is globally disabled.

Views

System view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN ID or a range of VLAN IDs in the form of *vlan-id1* to *vlan-id2*. The value range for VLAN IDs is 1 to 4094. The ID for *vlan-id2* must be equal to or greater than the ID for *vlan-id1*.

all: Specifies all existing VLANs.

Usage guidelines

You can enable loop detection globally or on a per-port basis. When a port receives a detection frame in any VLAN, the loop protection action is triggered on that port, regardless of whether loop detection is enabled on it.

Example

Globally enable loop detection for VLAN 10 through VLAN 20.

```
<Sysname> system-view
[System] loopback-detection global enable vlan 10 to 20
```

Related commands

display loopback-detection

loopback-detection enable

loopback-detection interval-time

Use **loopback-detection interval-time** to set the loop detection interval.

Use **undo loopback-detection interval-time** to restore the default.

Syntax

loopback-detection interval-time *interval*

undo loopback-detection interval-time

Default

The loop detection interval is 30 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Sets the loop detection interval in the range of 1 to 300 seconds.

Usage guidelines

With loop detection enabled, the device sends loop detection frames at the specified interval. A shorter interval offers more sensitive detection but consumes more resources. Consider the system performance and loop detection speed when you set the loop detection interval.

Example

Set the loop detection interval to 10 seconds.

```
<Sysname> system-view
[Sysname] loopback-detection interval-time 10
```

Related commands

display loopback-detection

loopback-detection led-flashing enable

Use **loopback-detection led-flashing enable** to enable LED flashing for loop detection.

Use **loopback-detection led-flashing enable** to disable LED flashing for loop detection.

NOTE:

This command is supported only by the S5000V3-EI, S5000V5-EI, S5000E-X, S5000X-EI, and WAS6100 switch series.

This command is supported only in Release 6328 and later.

Syntax

loopback-detection led-flashing enable

undo loopback-detection led-flashing enable

Default

LED flashing is disabled for loop detection.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

This command enables the device to flash port LEDs in Link/Active mode for loops when loop detection is enabled globally or on a per-port basis. When a loop is detected, port LEDs flash as follows:

- The LED for a looped port turns to steady green.
- The LEDs for unlooped ports turn to flashing green.

The device flashes port LEDs for a loop only when LED flashing is enabled on all ports that form the loop on the device. As a best practice, enable LED flashing for loop detection on all physically up Layer 2 interfaces.

Example

Enable LED flashing for loop detection on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] loopback-detection led-flashing enable
```

Contents

VLAN commands

Basic VLAN commands

bandwidth

Use **bandwidth** to set the expected bandwidth of an interface.

Use **undo bandwidth** to restore the default.

Syntax

bandwidth *bandwidth-value*

undo bandwidth

Default

The expected bandwidth (in kbps) is the interface baud rate divided by 1000.

Views

VLAN interface view

Predefined user roles

network-admin

Parameters

bandwidth-value: Specifies the expected bandwidth in the range of 1 to 400000000 kbps.

Usage guidelines

The expected bandwidth is an informational parameter used only by higher-layer protocols for calculation. You cannot adjust the actual bandwidth of an interface by using this command.

Examples

Set the expected bandwidth to 10000 kbps for VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] bandwidth 10000
```

default

Use **default** to restore the default settings for a VLAN interface.

Syntax

default

Views

VLAN interface view

Predefined user roles

network-admin

Usage guidelines

CAUTION:

The **default** command might interrupt ongoing network services. Make sure you are fully aware of the impact of this command when you use it on a live network.

This command might fail to restore the default settings for some commands for reasons such as command dependencies or system restrictions. Use the **display this** command in interface view to identify these commands, and then use their **undo** forms or follow the command reference to restore their default settings. If your restoration attempt still fails, follow the error message instructions to resolve the problem.

Examples

Restore the default settings for VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] default
```

description

Use **description** to configure the description of a VLAN or VLAN interface.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

For a VLAN, the description is **VLAN** *vlan-id*. The *vlan-id* argument specifies the VLAN ID in a four-digit format. If the VLAN ID has fewer than four digits, leading zeros are added. For example, the default description of VLAN 100 is **VLAN 0100**.

For a VLAN interface, the description is the name of the interface. For example, **Vlan-interface1 Interface**.

Views

VLAN view

VLAN interface view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 255 characters.

Usage guidelines

To manage VLANs and VLAN interfaces efficiently, configure descriptions for them based on their functions or connections.

Examples

Configure the description of VLAN 2 as **sales-private**.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] description sales-private
```

Configure the description of VLAN-interface 2 as **linktoPC56**.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] quit
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] description linktoPC56
```

Related commands

display interface vlan-interface

display vlan

display interface vlan-interface

Use **display interface vlan-interface** to display VLAN interface information.

Syntax

display interface [**vlan-interface** [*interface-number*]] [**brief** [**description** | **down**]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan-interface *interface-number*: Specifies a VLAN interface number. If you do not specify the **vlan-interface** keyword, the command displays information about all interfaces supported by the device. If you specify the **vlan-interface** keyword without specifying an interface number, the command displays information about all existing VLAN interfaces.

brief: Displays brief interface information. If you do not specify this keyword, the command displays detailed interface information.

description: Displays complete interface descriptions. If you do not specify this keyword, the command displays only the first 27 characters of each interface description.

down: Displays VLAN interfaces in down state and their down causes. If you do not specify this keyword, the command displays information about VLAN interfaces in all states.

Examples

Display information about VLAN-interface 10.

```
<Sysname> display interface vlan-interface 10
Vlan-interface10
Current state: UP
Line protocol state: UP
Description: Vlan-interface10 Interface
Bandwidth: 100000 kbps
Maximum transmission unit: 1500
Internet Address is 192.168.1.54/24 Primary
IP packet frame type: Ethernet II, hardware address: 0023-89b6-d613
IPv6 packet frame type: Ethernet II, hardware address: 0023-89b6-d613
Last clearing of counters: Never
```

Display brief information about VLAN-interface 2.

```
<Sysname> display interface vlan-interface 2 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP         Description
Vlan2                DOWN DOWN     --
```

Table 1 Command output

Field	Description
Vlan-interface2	VLAN interface name.
Current state	Physical link state of the VLAN interface: • **Administratively DOWN**—The interface has been shut down by using the **shutdown** command. • **DOWN**—The interface is administratively up, but its physical state is down. The VLAN of this VLAN interface does not contain any physical ports in up state. The ports might not be connected correctly or the links might have failed. • **UP**—The interface is both administratively and physically up.
Line protocol state	Data link layer state of the VLAN interface: • **DOWN**—The link layer protocol state of the interface is down. • **UP**—The link layer protocol state of the interface is up.
Description	Description of the VLAN interface.
Bandwidth	Expected bandwidth of the VLAN interface.
Maximum transmission unit	MTU of the VLAN interface.
Internet protocol processing : Disabled	The VLAN interface is not assigned an IP address and cannot process IP packets.
Internet Address	IP address of the VLAN interface. The **primary** attribute indicates that the address is the primary IP address.
IP packet frame type	IPv4 packet framing format.
hardware address	MAC address of the VLAN interface.
IPv6 packet frame type	IPv6 packet framing format.
Last clearing of counters	The most recent time that the **reset counters interface vlan-interface** command was executed. This field displays **Never** if you have never executed this command.
Brief information on interfaces in route mode	Brief information about Layer 3 interfaces.
Interface	Abbreviated interface name.
Link	Physical link state of the interface: • **UP**—The interface is physically up. • **DOWN**—The interface is physically down. • **ADM**—The interface has been shut down by using the **shutdown** command. To restore the physical state of the interface, use the **undo shutdown** command. • **Stby**—The interface is a backup interface in standby state.

Field	Description
	To see the primary interface, use the **display interface-backup state** command.
Protocol	Data link layer protocol state of the interface: • **UP**—The data link layer protocol state of the interface is up. • **DOWN**—The data link layer protocol state of the interface is down. • **UP(s)**—The data link layer protocol of the interface is up, but the link is an on-demand link or does not exist. The **(s)** attribute represents the spoofing flag.
Primary IP	Primary IP address of the interface.

Related commands

reset counters interface vlan-interface

display vlan

Use **display vlan** to display VLAN information.

Syntax

display vlan [*vlan-id1* [**to** *vlan-id2*] | **all** | **dynamic** | **reserved** | **static**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan-id1: Specifies a VLAN by its ID in the range of 1 to 4094.

vlan-id1 **to** *vlan-id2*: Specifies a VLAN ID range. Both the *vlan-id1* and the *vlan-id2* arguments are in the range of 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument.

all: Specifies all VLANs except the reserved VLANs.

dynamic: Specifies dynamic VLANs. If you specify this keyword, the command displays the total number of dynamic VLANs and each dynamic VLAN ID. Dynamic VLANs are generated through MVRP or assigned by a RADIUS server.

reserved: Specifies reserved VLANs. Protocol modules determine which VLANs are reserved according to function implementation. The reserved VLANs provide services for protocol modules. You cannot configure reserved VLANs.

static: Specifies static VLANs. If you specify this keyword, the command displays the total number of static VLANs and each static VLAN ID. Static VLANs are manually created.

Examples

Display information about VLAN 2.

```
<Sysname> display vlan 2
 VLAN ID: 2
 VLAN type: Static
```

```
 Route interface: Not configured
 Description: VLAN 0002
 Name: VLAN 0002
 Tagged ports:   None
 Untagged ports:
    GigabitEthernet1/0/1  GigabitEthernet1/0/2  GigabitEthernet1/0/3
```

Display information about VLAN 3.

```
<Sysname> display vlan 3
 VLAN ID: 3
 VLAN type: static
 Route interface: Configured
 IPv4 address: 1.1.1.1
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0003
 Name: VLAN 0003
 Tagged ports:   None
 Untagged ports: None
```

Table 2 Command output

Field	Description
VLAN type	VLAN type, static or dynamic.
Route interface	Whether the VLAN interface is configured for the VLAN. • Not configured. • Configured.
Description	Description of the VLAN.
Name	VLAN name.
IP address	Primary IPv4 address of the VLAN interface. This field is displayed only when an IPv4 address is configured for the VLAN interface. When the VLAN interface is also configured with secondary IPv4 addresses, you can view them by using one of the following commands: • **display interface vlan-interface**. • **display this** (VLAN interface view).
Subnet mask	Subnet mask of the primary IP address. This field is available only when an IP address is configured for the VLAN interface.
Tagged ports	Tagged members of the VLAN.
Untagged ports	Untagged members of the VLAN.

Related commands

vlan

display vlan brief

Use **display vlan brief** to display brief VLAN information.

Syntax

`display vlan brief`

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display brief VLAN information.

```
<Sysname> display vlan brief
Brief information about all VLANs:
Supported Minimum VLAN ID: 1
Supported Maximum VLAN ID: 4094
Default VLAN ID: 1
VLAN ID   Name                                Port
1         VLAN 0001                           GE1/0/1  GE1/0/2  GE1/0/3  GE1/0/4
                                              GE1/0/5  GE1/0/6  GE1/0/7  GE1/0/8
                                              GE1/0/9  GE1/0/10  GE1/0/11
                                              GE1/0/12  GE1/0/13  GE1/0/14
                                              GE1/0/15  GE1/0/16  GE1/0/17
                                              GE1/0/18  GE1/0/19  GE1/0/20
                                              GE1/0/21  GE1/0/22  GE1/0/23
                                              GE1/0/24  GE1/0/25  GE1/0/26
                                              GE1/0/27  GE1/0/28  GE1/0/29
                                              GE1/0/30  GE1/0/31  GE1/0/32
                                              GE1/0/33  GE1/0/34  GE1/0/35
                                              GE1/0/36  GE1/0/37  GE1/0/38
                                              GE1/0/39  GE1/0/40  GE1/0/41
                                              GE1/0/42  GE1/0/43  GE1/0/44
                                              GE1/0/45  GE1/0/46  GE1/0/47
                                              GE1/0/48
2         VLAN 0002
3         VLAN 0003
```

Table 3 Command output

Field	Description
Default VLAN ID	System default VLAN ID.
Name	VLAN name.
Port	Ports that allow packets from the VLAN to pass through.

interface vlan-interface

Use **`interface vlan-interface`** to create a VLAN interface and enter its view, or enter the view of an existing VLAN interface.

Use **undo interface vlan-interface** to delete a VLAN interface.

Syntax

interface vlan-interface *interface-number*

undo interface vlan-interface *interface-number*

Default

No VLAN interfaces exist.

Views

System view

Predefined user roles

network-admin

Parameters

interface-number: Specifies a VLAN interface number in the range of 1 to 4094.

Usage guidelines

Create the VLAN before you create the VLAN interface for a VLAN.

You cannot create VLAN interfaces for secondary VLANs that meet the following requirements:

- Associated with the same primary VLAN.
- Enabled with Layer 3 communication in VLAN interface view of the primary VLAN interface.

Examples

Create VLAN-interface 2, and enter its view.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] quit
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2]
```

Related commands

display interface vlan-interface

mtu

Use **mtu** to set the MTU for a VLAN interface.

Use **undo mtu** to restore the default.

Syntax

mtu *size*

undo mtu

Default

The MTU of a VLAN interface is 1500 bytes.

Views

VLAN interface view

Predefined user roles

network-admin

Parameters

size: Sets the MTU in bytes. The value range for this argument is 128 to 1500.

Usage guidelines

If you configure both the **mtu** and **ip mtu** commands on a VLAN interface, the MTU set by the **ip mtu** command is used for fragmentation. For more information about the **ip mtu** command, see *Layer 3—IP Services Command Reference*.

Examples

Set the MTU to 1492 bytes for VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] mtu 1492
```

Related commands

display interface vlan-interface

name

Use **name** to assign a name to a VLAN.

Use **undo name** to restore the default.

Syntax

name *text*

undo name

Default

The name of a VLAN is **VLAN** *vlan-id.* The *vlan-id* argument specifies the VLAN ID in a four-digit format. If the VLAN ID has fewer than four digits, leading zeros are added. For example, the name of VLAN 100 is **VLAN 0100**.

Views

VLAN view

Predefined user roles

network-admin

Parameters

text: Specifies a VLAN name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

For 802.1X or MAC authentication, you can specify authorization VLANs by their names or IDs. If a large number of VLANs are configured, use VLAN names to identify them.

Examples

Assign the name **test vlan** to VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] name test vlan
```

Related commands

display vlan

reset counters interface vlan-interface

Use **reset counters interface vlan-interface** to clear statistics on a VLAN interface.

Syntax

reset counters [interface vlan-interface [*interface-number*]]

Views

User view

Predefined user roles

network-admin

Parameters

vlan-interface *interface-number*: Specifies a VLAN interface by its number. If you do not specify the **vlan-interface** keyword, the command clears statistics on all interfaces. If you specify the **vlan-interface** keyword without specifying an interface number, the command clears statistics on all existing VLAN interfaces.

Usage guidelines

Use this command to clear the history statistics before you collect statistics within a time period.

Examples

Clear statistics on VLAN-interface 2.

```
<Sysname> reset counters interface vlan-interface 2
```

Related commands

display interface vlan-interface

shutdown

Use **shutdown** to shut down a VLAN interface.

Use **undo shutdown** to bring up a VLAN interface.

Syntax

shutdown

undo shutdown

Default

A VLAN interface is not manually shut down, and the following guidelines apply to the interface state:

- The VLAN interface is down if all ports in the VLAN are down.
- The VLAN interface is up if one or more ports in the VLAN are up.

Views

VLAN interface view

Predefined user roles

network-admin

Usage guidelines

CAUTION:

Executing the **shutdown** command on a VLAN interface will disconnect the link of the VLAN interface and interrupt communication. Use this command with caution.

When you use this command to shut down a VLAN interface, the VLAN interface remains in DOWN (Administratively) state. In this case, the VLAN interface state is not affected by the state of the ports in the VLAN.

Before you configure parameters for a VLAN interface, use this command to shut it down to prevent the configuration from affecting the network. After you complete the VLAN interface configuration, use the **undo shutdown** command to make the settings take effect.

To troubleshoot a failed VLAN interface, you can use the **shutdown** command and then the **undo shutdown** command on the interface to see whether it recovers.

In a VLAN, the state of each Ethernet port is independent of the state of the VLAN interface.

Examples

Shut down VLAN-interface 2, and then bring it up.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] shutdown
[Sysname-Vlan-interface2] undo shutdown
```

vlan

Use **vlan** *vlan-id-list* to create VLANs in batches, except reserved VLANs.

Use **vlan all** to create VLANs 1 through 4094.

Use **undo vlan** to delete the specified VLANs.

Syntax

vlan { *vlan-id-list* | **all** }

undo vlan { *vlan-id-list* | **all** }

Default

VLAN 1 (system default VLAN) exists.

Views

System view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 32 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* [**to** *vlan-id2*]. The value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

all: Specifies all VLANs except reserved VLANs. The keyword is not supported when the maximum number of VLANs that can be created on a device is less than 4094.

Usage guidelines

You cannot create or delete the system default VLAN (VLAN 1) or reserved VLANs.

Before you delete a dynamic VLAN or a VLAN locked by an application, you must first remove the configuration from the VLAN.

Examples

Create VLAN 2 and enter its view.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2]
```

Create VLAN 2 and VLANs 4 through 100.

```
<Sysname> system-view
[Sysname] vlan 2 4 to 100
```

Related commands

`display vlan`

Port-based VLAN commands

display port

Use **`display port`** to display information about hybrid or trunk ports.

Syntax

`display port` { **`hybrid`** | **`trunk`** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

`hybrid`: Specifies hybrid ports.

`trunk`: Specifies trunk ports.

Examples

Display information about hybrid ports.

```
<Sysname> display port hybrid
Interface            PVID  VLAN Passing
GE1/0/1              100   Tagged:  1000, 1002, 1500, 1600-1611, 2000,
                                    2555-2558, 3000, 4000
                           Untagged:1, 10, 15, 18, 20-30, 44, 55, 67, 100,
                                    150-160, 200, 255, 286, 300-302
```

Display information about trunk ports.

```
<Sysname> display port trunk
Interface            PVID  VLAN Passing
GE1/0/2              2     1-4, 6-100, 145, 177, 189-200, 244, 289, 400,
```

```
555, 600-611, 1000, 2006-2008
```

Table 4 Command output

Field	Description
Interface	Interface name.
PVID	Port VLAN ID.
VLAN Passing	Existing VLANs allowed on the port.
Tagged	VLANs from which the port sends packets without removing VLAN tags.
Untagged	VLANs from which the port sends packets after removing VLAN tags.

port

Use **port** to assign the specified access ports to a VLAN.

Use **undo port** to remove the specified access ports from a VLAN.

Syntax

port *interface-list*

undo port *interface-list*

Default

All ports are in VLAN 1.

Views

VLAN view

Predefined user roles

network-admin

Parameters

interface-list: Specifies a space-separated list of up to 10 Ethernet interface items. Each item specifies an Ethernet interface or a range of Ethernet interfaces in the form of *interface-type interface-number1* **to** *interface-type interface-number2*. The value for the *interface-number2* argument must be equal to or greater than the value for the *interface-number1* argument.

Usage guidelines

This command is applicable only to access ports. This command is not supported in the view of VLAN 1.

By default, all ports are access ports. You can manually configure the port link type. For more information, see "port link-type."

Examples

Assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

Related commands

display vlan

port access vlan

Use **port access vlan** to assign an access port to the specified VLAN.

Use **undo port access vlan** to restore the default.

Syntax

port access vlan *vlan-id*

undo port access vlan

Default

All access ports belong to VLAN 1.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies a VLAN by its ID in the range of 1 to 4094.

Usage guidelines

By default, all access ports belong to VLAN 1. Therefore, this command cannot be used to assign access ports to VLAN 1. To move an access port to VLAN 1, execute the **undo port access vlan** command on the access port.

Before assigning an access port to a VLAN, make sure the VLAN has been created.

Examples

Assign GigabitEthernet 1/0/1 to VLAN 3.

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port access vlan 3
```

port hybrid pvid

Use **port hybrid pvid** to set the PVID of a hybrid port.

Use **undo port hybrid pvid** to set the PVID of a hybrid port to 1.

Syntax

port hybrid pvid vlan *vlan-id*

undo port hybrid pvid

Default

The PVID of a hybrid port is the ID of the VLAN to which the port belongs when its link type is **access**.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies a VLAN by its ID in the range of 1 to 4094.

Usage guidelines

You can use a nonexistent VLAN as the PVID of a hybrid port. When you delete the PVID of a hybrid port by using the **undo vlan** command, the PVID setting of the port does not change.

For correct packet transmission, set the same PVID for a local hybrid port and its peer.

To enable a hybrid port to transmit packets from its PVID, you must assign the hybrid port to the PVID by using the **port hybrid vlan** command.

Examples

Configure GigabitEthernet 1/0/1 as a hybrid port, set its PVID to VLAN 100, and assign it to VLAN 100 as an untagged member.

```
<Sysname> system-view
[Sysname] vlan 100
[Sysname-vlan100] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type hybrid
[Sysname-GigabitEthernet1/0/1] port hybrid pvid vlan 100
[Sysname-GigabitEthernet1/0/1] port hybrid vlan 100 untagged
```

Related commands

port hybrid vlan

port link-type

port hybrid vlan

Use **port hybrid vlan** to assign a hybrid port to the specified VLANs.

Use **undo port hybrid vlan** to remove a hybrid port from the specified VLANs.

Syntax

port hybrid vlan *vlan-id-list* { **tagged** | **untagged** }

undo port hybrid vlan *vlan-id-list*

Default

A hybrid port is an untagged member of the VLAN to which the port belongs when its link type is **access**.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 32 VLAN items. Each item specifies a VLAN ID or a range of VLAN IDs in the form of *vlan-id1* **to** *vlan-id2*. The value range for VLAN IDs is 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument. The specified VLANs must already exist on the device.

tagged: Configures the port as a tagged member of the specified VLANs. A tagged member of a VLAN sends packets from the VLAN without removing VLAN tags.

untagged: Configures the port as an untagged member of the specified VLANs. An untagged member of a VLAN sends packets from the VLAN after removing VLAN tags.

Usage guidelines

A hybrid port can allow multiple VLANs. If you execute this command multiple times on a hybrid port, the hybrid port allows all the specified VLANs.

Examples

Configure GigabitEthernet 1/0/1 as a hybrid port, and assign it to VLAN 2, VLAN 4, and VLAN 50 through VLAN 100 as a tagged member.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type hybrid
[Sysname-GigabitEthernet1/0/1] port hybrid vlan 2 4 50 to 100 tagged
```

Related commands

port link-type

port link-type

Use **port link-type** to set the link type of a port.

Use **undo port link-type** to restore the default link type of a port.

Syntax

port link-type { **access** | **hybrid** | **trunk** }

undo port link-type

Default

Each port is an access port.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

access: Sets the port link type to access.

hybrid: Sets the port link type to hybrid.

trunk: Sets the port link type to trunk.

Usage guidelines

To change the link type of a port from trunk to hybrid or vice versa, first set the link type to access.

Examples

Configure GigabitEthernet 1/0/1 as a trunk port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
```

port trunk permit vlan

Use **port trunk permit vlan** to assign a trunk port to the specified VLANs.

Use **undo port trunk permit vlan** to remove a trunk port from the specified VLANs.

Syntax

port trunk permit vlan { *vlan-id-list* | **all** }

undo port trunk permit vlan { *vlan-id-list* | **all** }

Default

A trunk port allows packets only from VLAN 1 to pass through.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 32 VLAN items. Each item specifies a VLAN ID or a range of VLAN IDs in the form of *vlan-id1* **to** *vlan-id2*. The value range for VLAN IDs is 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument.

all: Specifies all VLANs. To prevent unauthorized VLAN users from accessing restricted resources through the port, use the **port trunk permit vlan all** command with caution.

Usage guidelines

A trunk port can allow multiple VLANs. If you execute this command multiple times on a trunk port, the trunk port allows all the specified VLANs.

On a trunk port, packets only from the PVID can pass through untagged.

Examples

Configure GigabitEthernet 1/0/1 as a trunk port, and assign it to VLAN 2, VLAN 4, and VLAN 50 through VLAN 100.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
[Sysname-GigabitEthernet1/0/1] port trunk permit vlan 2 4 50 to 100
```

Related commands

port link-type

port trunk pvid

Use **port trunk pvid** to set the PVID for a trunk port.

Use **undo port trunk pvid** to restore the default.

Syntax

port trunk pvid vlan *vlan-id*

undo port trunk pvid

Default

The PVID of a trunk port is VLAN 1.

Views

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies a VLAN by its ID in the range of 1 to 4094.

Usage guidelines

You can use a nonexistent VLAN as the PVID for a trunk port. When you delete the PVID of a trunk port by using the **undo vlan** command, the PVID setting of the port does not change.

For correct packet transmission, set the same PVID for a local trunk port and its peer.

To enable a trunk port to transmit packets from its PVID, you must assign the trunk port to the PVID by using the **port trunk permit vlan** command.

Examples

Configure GigabitEthernet 1/0/1 as a trunk, set its PVID to VLAN 100, and assign it to VLAN 100.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
[Sysname-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Sysname-GigabitEthernet1/0/1] port trunk permit vlan 100
```

Related commands

port link-type

port trunk permit vlan

MAC-based VLAN commands

display mac-vlan

Use **display mac-vlan** to display MAC-to-VLAN entries.

Syntax

display mac-vlan { **all** | **dynamic** | **mac-address** *mac-address* [**mask** *mac-mask*] | **static** | **vlan** *vlan-id* }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

all: Specifies all MAC-to-VLAN entries.

dynamic: Specifies dynamically configured MAC-to-VLAN entries.

mac-address *mac-address*: Specifies the MAC address in the MAC-to-VLAN entry. The format of the *mac-address* argument is H-H-H.

mask *mac-mask*: Specifies the mask for matching MAC addresses in MAC-to-VLAN entries. For the *mac-mask* argument, the high-order bits must be consecutive 1s in binary notation or consecutive Fs in hexadecimal notation. The default value is ffff-ffff-ffff.

static: Specifies statically configured MAC-to-VLAN entries.

vlan *vlan-id*: Specifies the VLAN in MAC-to-VLAN entries. The value range for the *vlan-id* argument is 1 to 4094.

Examples

Display all MAC-to-VLAN entries.

```
<Sysname> display mac-vlan all
The following MAC VLAN entries exist:
State: S - Static, D - Dynamic

MAC address        Mask               VLAN ID   Dot1p      State
0008-0001-0000     ffff-ff00-0000     5         3          S
0002-0001-0000     ffff-ffff-ffff     5         3          S&D

Total MAC VLAN entries count: 2
```

Table 5 Command output

Field	Description
S - Static	Statically configured MAC-to-VLAN entries.
D - Dynamic	Dynamically configured MAC-to-VLAN entries.
MAC address	MAC address of the MAC-to-VLAN entry.
Mask	MAC address mask of the MAC-to-VLAN entry.
VLAN ID	VLAN ID of the MAC-to-VLAN entry.
Dot1p	802.1p priority of the VLAN in the MAC-to-VLAN entry.
State	State of a MAC-to-VLAN entry: • **S**—The MAC-to-VLAN entry is configured statically. • **D**—The MAC-to-VLAN entry is dynamically issued by the authentication server. • **S&D**—The MAC-to-VLAN entry is configured both statically and dynamically.

Related commands

mac-vlan mac-address

display mac-vlan interface

Use **display mac-vlan interface** to display all ports that are enabled with the MAC-based VLAN feature.

Syntax

display mac-vlan interface

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display all ports that are enabled with the MAC-based VLAN feature.

```
<Sysname> display mac-vlan interface
MAC VLAN is enabled on following ports:
GigabitEthernet1/0/1  GigabitEthernet1/0/2  GigabitEthernet1/0/3
```

Related commands

mac-vlan enable

mac-vlan enable

Use **mac-vlan enable** to enable the MAC-based VLAN feature on a port.

Use **undo mac-vlan enable** to disable the MAC-based VLAN feature on a port.

Syntax

mac-vlan enable

undo mac-vlan enable

Default

The MAC-based VLAN feature is disabled on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Examples

Enable the MAC-based VLAN feature on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname–GigabitEthernet1/0/1] mac-vlan enable
```

Related commands

display mac-vlan interface

mac-vlan mac-address

Use **mac-vlan mac-address** to configure a MAC-to-VLAN entry.

Use **undo mac-vlan** to delete the specified MAC-to-VLAN entries.

Syntax

mac-vlan mac-address *mac-address* [**mask** *mac-mask*] **vlan** *vlan-id* [**dot1p** *priority*]

undo mac-vlan { **all** | **mac-address** *mac-address* [**mask** *mac-mask*] | **vlan** *vlan-id* }

Default

No MAC-to-VLAN entries exist.

Views

System view

Predefined user roles

network-admin

Parameters

mac-address *mac-address*: Specifies a MAC address in the format of H-H-H. The MAC address cannot be a multicast MAC address or all 0s. When you configure a MAC address, leading zeros in each H section can be omitted. For example, to configure a MAC address 000f-00e2-0001, you can enter only **f-e2-1**.

mask *mac-mask*: Specifies the MAC address mask. For the *mac-mask* argument, the high-order bits must be consecutive 1s in binary notation or consecutive Fs in hexadecimal notation. The default value is ffff-ffff-ffff.

vlan *vlan-id*: Specifies a VLAN ID in the range of 1 to 4094.

dot1p *priority*: Specifies the 802.1p priority of the VLAN specific to the MAC-to-VLAN entry. The value range for the *priority* argument is 0 to 7, and the default value is 0. The higher the value, the higher the 802.1p priority.

all: Specifies all static MAC-to-VLAN entries.

Usage guidelines

For successful dynamic MAC-based VLAN assignment, use static VLANs when you create MAC-to-VLAN entries.

Different types of MAC-to-VLAN entries are created depending on whether you specify the **mask** keyword.

- When you specify this keyword, the created MAC-to-VLAN entry describes the relationship among a group of MAC addresses, a VLAN, and the 802.1p priority for the VLAN.
- When you do not specify this keyword, the created MAC-to-VLAN entry describes the relationship among a MAC address, a VLAN, and the 802.1p priority for the VLAN.

These different types of MAC-to-VLAN entries are stored separately in two tables. The system updates the two tables according to the configuration.

Examples

Associate the MAC address 0000-0001-0001 with VLAN 100, and set the 802.1p priority to 7 for VLAN 100 in this entry.

```
<Sysname> system-view
[Sysname] mac-vlan mac-address 0-1-1 vlan 100 dot1p 7
```

Associate VLAN 100 with MAC addresses whose six high-order bits are 121122, and set the 802.1p priority to 4 for VLAN 100 in this entry.

```
<Sysname> system-view
[Sysname] mac-vlan mac-address 1211-2222-3333 mask ffff-ff00-0000 vlan 100 dot1p 4
```

Related commands

display mac-vlan

mac-vlan trigger enable

Use **mac-vlan trigger enable** to enable dynamic MAC-based VLAN assignment on a port.

Use **undo mac-vlan trigger enable** to disable dynamic MAC-based VLAN assignment on a port.

Syntax

mac-vlan trigger enable

undo mac-vlan trigger enable

Default

Dynamic MAC-based VLAN assignment is disabled on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

VLAN assignment for a port is triggered only when the source MAC address of its received packet exactly matches the MAC address in a MAC-to-VLAN entry.

Examples

Enable dynamic MAC-based VLAN assignment on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-vlan trigger enable
```

Related commands

mac-vlan mac-address

port pvid forbidden

port pvid forbidden

Use **port pvid forbidden** to disable a port from forwarding packets that fail the exact MAC address match in its PVID.

Use **undo port pvid forbidden** to restore the default.

Syntax

port pvid forbidden

undo port pvid forbidden

Default

When a port receives packets whose source MAC addresses fail the exact MAC address match, the port forwards them in its PVID.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

Use this feature only with dynamic MAC-based VLAN assignment.

Examples

Disable GigabitEthernet 1/0/1 from forwarding packets that fail the exact MAC address match in its PVID.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port pvid forbidden
```

Related commands

mac-vlan trigger enable

vlan precedence

Use **vlan precedence** to set the VLAN matching order.

Use **undo vlan precedence** to restore the default.

Syntax

vlan precedence { **mac-vlan** | **ip-subnet-vlan** }

undo vlan precedence

Default

A port matches VLANs based on MAC addresses preferentially.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

mac-vlan: Matches VLANs based on MAC addresses preferentially.

ip-subnet-vlan: Matches VLANs based on IP subnets preferentially.

Usage guidelines

This command takes effect only on MAC-based VLANs and IP subnet-based VLANs.

When you enable dynamic MAC-based VLAN assignment, configure the **vlan precedence mac-vlan** command as a best practice to ensure the priority of MAC-based VLAN matching. If you execute the **vlan precedence ip-subnet-vlan** command, the command does not take effect.

Examples

Configure GigabitEthernet 1/0/1 to match VLANs based on MAC addresses preferentially.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] vlan precedence mac-vlan
```

Related commands

mac-vlan trigger enable

IP subnet-based VLAN commands

display ip-subnet-vlan interface

Use **display ip-subnet-vlan interface** to display IP subnet-based VLANs that are associated with the specified ports.

Syntax

display ip-subnet-vlan interface { *interface-type interface-number1* [**to** *interface-type interface-number2*] | **all** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number1 **to** *interface-type interface-number2*: Specifies an interface range. Both the *interface-type interface-number1* argument and the *interface-type interface-number2* argument represent the interface type and interface number. The value for the *interface-number2* argument must be greater than or equal to the value for the *interface-number1* argument.

all: Specifies all ports.

Examples

Display IP subnet-based VLANs on GigabitEthernet 1/0/1.

```
<Sysname> display ip-subnet-vlan interface gigabitethernet 1/0/1
 Interface: GigabitEthernet1/0/1
  VLAN ID   Subnet index    IP address       Subnet mask       Status
  3         0               192.168.1.0      255.255.255.0     Active
  4         N/A             N/A              N/A               Inactive
  4094      65535           172.16.1.1       255.255.0.0       Inactive
```

Table 6 Command output

Field	Description
VLAN ID	ID of the IP subnet-based VLAN.
Subnet index	Index of the IP subnet. This field displays **N/A** if no IP subnet-based VLAN is configured.
IP address	IP address of the subnet. It can be an IP address or a subnet address. This field displays **N/A** if no IP subnet address is configured for the VLAN.
Subnet mask	Mask of the IP subnet. This field displays **N/A** if no subnet mask is configured for the VLAN.

Status	Whether the IP subnet-based VLAN has taken effect on the port:
	• **Active**—The IP subnet-based VLAN has taken effect.
	• **Inactive**—The IP subnet-based VLAN has not taken effect. For example, this field displays **Inactive** in one of the following conditions:
	  ○ The configuration of the IP subnet-based VLAN is not complete.
	  ○ The port does not allow the IP subnet-based VLAN.

Related commands

`display ip-subnet-vlan vlan`

`ip-subnet-vlan`

`port hybrid ip-subnet-vlan`

display ip-subnet-vlan vlan

Use **`display ip-subnet-vlan vlan`** to display information about IP subnet-based VLANs.

Syntax

`display ip-subnet-vlan vlan` { *`vlan-id1`* [**`to`** *`vlan-id2`*] | **`all`** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

`vlan-id1`: Specifies an IP subnet-based VLAN by its VLAN ID in the range of 1 to 4094.

`vlan-id1` **`to`** *`vlan-id2`*: Specifies an IP subnet-based VLAN ID range. Both the *`vlan-id1`* and the *`vlan-id2`* arguments are in the range of 1 to 4094. The value for the *`vlan-id2`* argument must be equal to or greater than the value for the *`vlan-id1`* argument.

`all`: Specifies all IP subnet-based VLANs.

Examples

Display information about all IP subnet-based VLANs.

```
<Sysname> display ip-subnet-vlan vlan all
 VLAN ID: 3
  Subnet index      IP address      Subnet mask
```

```
0                   192.168.1.0     255.255.255.0
```

Table 7 Command output

Field	Description
VLAN ID	ID of the IP subnet-based VLAN.
Subnet index	Index of the IP subnet.
IP address	IP address of the subnet. It can be an IP address or a subnet address.
Subnet mask	Mask of the IP subnet.

Related commands

display ip-subnet-vlan interface

ip-subnet-vlan

port hybrid ip-subnet-vlan

ip-subnet-vlan

Use **ip-subnet-vlan** to associate a VLAN with the specified IP subnet or IP address.

Use **undo ip-subnet-vlan** to disassociate a VLAN from the specified IP subnet or IP address.

Syntax

ip-subnet-vlan [*ip-subnet-index*] **ip** *ip-address* [*mask*]

undo ip-subnet-vlan { *ip-subnet-index* [**to** *ip-subnet-end*] | **all** }

Default

A VLAN is not associated with an IP subnet or IP address.

Views

VLAN view

Predefined user roles

network-admin

Parameters

ip-subnet-index: Specifies a beginning IP subnet index in the range of 0 to 65535. The value can be configured by users. It can also be automatically numbered by the system based on the order in which the IP subnets or IP addresses are associated with the VLAN.

ip *ip-address* [*mask*]: Specifies the source IP address or network address that is associated with the VLAN. The *ip-address* argument specifies the source IP address or network address in dotted decimal notation. The *mask* argument is the subnet mask of the source IP address or network address, in dotted decimal notation with a default value of 255.255.255.0.

to *ip-subnet-end*: Specifies an end IP subnet index of an IP subnet index range, in the range of 0 to 65535. The value for the *ip-subnet-end* argument must be greater than or equal to the beginning IP subnet index.

all: Specifies all IP subnets or IP addresses that are associated with the VLAN.

Usage guidelines

The IP subnet or IP address cannot be a multicast network segment or a multicast address.

Examples

Configure VLAN 3 as an IP subnet-based VLAN and associate it with the subnet 192.168.1.0/24.

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] ip-subnet-vlan ip 192.168.1.0 255.255.255.0
```

Related commands

display ip-subnet-vlan interface

display ip-subnet-vlan vlan

port hybrid ip-subnet-vlan

port hybrid ip-subnet-vlan

Use **port hybrid ip-subnet-vlan** to associate a port with the specified IP subnet-based VLAN.

Use **undo port hybrid ip-subnet-vlan** to disassociate a port from the specified IP subnet-based VLAN.

Syntax

port hybrid ip-subnet-vlan vlan *vlan-id*

undo port hybrid ip-subnet-vlan { **vlan** *vlan-id* | **all** }

Default

A port is not associated with an IP subnet-based VLAN.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan *vlan-id*: Specifies a VLAN by its ID in the range of 1 to 4094.

all: Specifies all VLANs.

Usage guidelines

For this command to take effect, perform the following tasks:

1. Create a VLAN and associate it with the specified IP subnet or IP address.
2. Set the port link type to hybrid.
3. Configure the port to allow the IP subnet-based VLAN to pass through.

Examples

Associate GigabitEthernet 1/0/1 with IP subnet-based VLAN 3.

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] ip-subnet-vlan ip 192.168.1.0 255.255.255.0
[Sysname-vlan3] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type hybrid
```

```
[Sysname-GigabitEthernet1/0/1] port hybrid vlan 3 untagged
[Sysname-GigabitEthernet1/0/1] port hybrid ip-subnet-vlan vlan 3
```

Associate Layer 2 aggregate interface Bridge-Aggregation 1 with IP subnet-based VLAN 3.

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] ip-subnet-vlan ip 192.168.1.0 255.255.255.0
[Sysname-vlan3] quit
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port link-type hybrid
[Sysname-Bridge-Aggregation1] port hybrid vlan 3 untagged
[Sysname-Bridge-Aggregation1] port hybrid ip-subnet-vlan vlan 3
```

Related commands

display ip-subnet-vlan interface

display ip-subnet-vlan vlan

ip-subnet-vlan

Protocol-based VLAN commands

S5110V2-SI, S5000V3-EI, S5000V5-EI, S5000E-X, S5000X-EI, WAS6000 switches do not support protocol-based VLAN.

display protocol-vlan interface

Use **display protocol-vlan interface** to display protocol-based VLANs that are associated with the specified ports.

Syntax

display protocol-vlan interface { *interface-type interface-number1* [**to** *interface-type interface-number2*] | **all** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number1 **to** *interface-type interface-number2*: Specifies an interface range. Both the *interface-type interface-number1* argument and the *interface-type interface-number2* argument represent the interface type and interface number. The value for the *interface-number2* argument must be greater than or equal to the value for the *interface-number1* argument.

all: Specifies all ports.

Examples

Display protocol-based VLAN information on GigabitEthernet 1/0/1.

```
<Sysname> display protocol-vlan interface gigabitethernet 1/0/1
 Interface: GigabitEthernet1/0/1
```

```
VLAN ID  Protocol index  Protocol type            Status
2        0               IPv6                     Active
2        1               N/A                      Inactive
4094     65535           IPv4                     Inactive
```

Table 8 Command output

Field	Description
VLAN ID	ID of the protocol-based VLAN.
Protocol index	Protocol template index.
Protocol type	Protocol type specified by the protocol template. This field displays **N/A** if the protocol type is not specified.
Status	Whether the protocol-based VLAN has taken effect: • **Active**—The protocol-based VLAN has taken effect. • **Inactive**—The protocol-based VLAN has not taken effect.

Related commands

display protocol-vlan vlan

port hybrid protocol-vlan

protocol-vlan

display protocol-vlan vlan

Use **display protocol-vlan vlan** to display information about protocol-based VLANs.

Syntax

display protocol-vlan vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan-id1: Specifies a protocol-based VLAN ID in the range of 1 to 4094.

vlan-id1 **to** *vlan-id2:* Specifies a protocol-based VLAN ID range. Both the *vlan-id1* and the *vlan-id2* arguments are in the range of 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument.

all: Specifies all protocol-based VLANs.

Examples

Displays information about all protocol-based VLANs.

```
<Sysname> display protocol-vlan vlan all
 VLAN ID: 2
  Protocol index  Protocol type
  0               IPv4
  65535           IPv6
```

```
VLAN ID: 3
 Protocol index  Protocol type
 0               IPv4
 65535           LLC DSAP 0x11 SSAP 0x22
```

Table 9 Command output

Field	Description
VLAN ID	ID of the protocol-based VLAN.
Protocol index	Protocol template index.
Protocol type	Protocol type or encapsulation format specified by the protocol template.

Related commands

display protocol-vlan interface

port hybrid protocol-vlan

protocol-vlan

port hybrid protocol-vlan

Use **port hybrid protocol-vlan** to associate a port with the specified protocol-based VLAN.

Use **undo port hybrid protocol-vlan** to disassociate a port from the specified protocol-based VLAN.

Syntax

port hybrid protocol-vlan vlan *vlan-id* { *protocol-index* [**to** *protocol-end*] | **all** }

undo hybrid protocol-vlan { **vlan** *vlan-id* { *protocol-index* [**to** *protocol-end*] | **all** } | **all** }

Default

A port is not associated with a protocol-based VLAN.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan *vlan-id*: Specifies a VLAN by its ID in the range of 1 to 4094.

protocol-index: Specifies a beginning protocol template index in the range of 0 to 65535.

to *protocol-end*: Specifies an end protocol template index of a protocol template range, in the range of 0 to 65535. The value for this argument must be greater than or equal to the beginning protocol template index.

all: Specifies all protocol templates.

Usage guidelines

For this command to take effect, perform the following tasks:

1. Create a VLAN and associate it with the specified protocol templates.
2. Set the port link type to hybrid.
3. Configure the port to allow the protocol-based VLAN to pass through.

When you execute the **undo port hybrid protocol-vlan** command on a port, follow these guidelines:

- If you specify both the *vlan-id* argument and the **all** keyword, this command disassociates the port from all protocol templates of the specified VLAN.
- If you specify only the **all** keyword, this command disassociates the port from all protocol templates of all VLANs.

Examples

Configure GigabitEthernet 1/0/1 as a hybrid port, assign it to VLAN 2 as an untagged member, and associated it with protocol template 1 in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] protocol-vlan 1 ipv4
[Sysname-vlan2] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type hybrid
[Sysname-GigabitEthernet1/0/1] port hybrid vlan 2 untagged
[Sysname-GigabitEthernet1/0/1] port hybrid protocol-vlan vlan 2 1
```

Configure Layer 2 aggregate interface Bridge-Aggregation 1 as a hybrid port, assign it to VLAN 2 as an untagged member, and associated it with protocol template 1 in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] protocol-vlan 1 ipv4
[Sysname-vlan2] quit
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port link-type hybrid
[Sysname-Bridge-Aggregation1] port hybrid vlan 2 untagged
[Sysname-Bridge-Aggregation1] port hybrid protocol-vlan vlan 2 1
```

protocol-vlan

Use **protocol-vlan** to associate a VLAN with the specified protocol template.

Use **undo protocol-vlan** to disassociate a VLAN from the specified protocol template.

Syntax

protocol-vlan [*protocol-index*] { **at** | **ipv4** | **ipv6** | **ipx** { **ethernetii** | **llc** | **raw** | **snap** } | **mode** { **ethernetii etype** *etype-id* | **llc** { **dsap** *dsap-id* [**ssap** *ssap-id*] | **ssap** *ssap-id* } | **snap etype** *etype-id* } }

undo protocol-vlan { *protocol-index* [**to** *protocol-end*] | **all** }

Default

A VLAN is not associated with a protocol template.

Views

VLAN view

Predefined user roles

network-admin

Parameters

at: Specifies the AppleTalk-based VLAN.

ipv4: Specifies the IPv4-based VLAN.

ipv6: Specifies the IPv6-based VLAN.

ipx: Specifies the IPX-based VLAN. The keywords **ethernetii**, **llc**, **raw**, and **snap** specify IPX encapsulation formats.

mode: Configures a user-defined protocol template for the VLAN. The keywords **ethernetii**, **llc**, and **snap** specify the available encapsulation formats.

ethernetii etype *etype-id*: Matches the Ethernet II encapsulation format and the specified protocol type ID. The *etype-id* argument specifies the protocol type ID of inbound packets, in the range of 600 to ffff in hexadecimal notation, excluding 800, 86dd, 809b, and 8137.

llc: Matches the LLC encapsulation format.

dsap *dsap-id*: Specifies the destination service access point in hexadecimal notation, in the range of 0 to ff.

ssap *ssap-id*: Specifies the source service access point in hexadecimal notation, in the range of 0 to ff.

snap etype *etype-id*: Matches the SNAP encapsulation format and the specified protocol type value. The *etype-id* argument specifies the Ethernet type of inbound packets, in the range of 600 to ffff in hexadecimal notation, excluding 8137.

protocol-index: Specifies a protocol template index that is associated with the VLAN. The value range for this argument is 0 to 65535. The system will automatically assign an index if you do not specify this argument.

to *protocol-end*: Specifies an end protocol template index of a protocol template range, in the range of 0 to 65535. The value for the *protocol-end* argument must be greater than or equal to the value for the *protocol-index* argument.

all: Specifies all protocols associated with the VLAN.

Usage guidelines

CAUTION:

IP uses ARP for address resolution in Ethernet. To prevent communication failures, configure the IP and ARP templates in the same VLAN and associate them with the same port.

When you use the **mode** keyword to configure a protocol template, follow these restrictions and guidelines:

- Do not set the *etype-id* argument in the **ethernetii etype** *etype-id* option to the following hexadecimal values:
  - **800**—Specifies the IPv4 protocol in Ethernet II encapsulation.
  - **809b**—Specifies the AppleTalk protocol in Ethernet II encapsulation.
  - **8137**—Specifies the IPX protocol in Ethernet II encapsulation.
  - **86dd**—Specifies the IPv6 protocol in Ethernet II encapsulation.

- Do not set both the *dsap-id* and *ssap-id* arguments to any of the following hexadecimal values:
  - **e0**—Specifies the 802.2 LLC encapsulation format for IPX packets.
  - **ff**—Specifies the 802.3 raw encapsulation format for IPX packets.
  - **aa**—Specifies the 802.2 SNAP encapsulation format.

  When either of the *dsap-id* and *ssap-id* arguments is configured, the system assigns the hexadecimal value **aa** to the other argument.
- Do not set the *etype-id* argument in the **snap etype** *etype-id* option to the hexadecimal value 8137. Otherwise, the template format will be the same as that of the IPX protocol. You can set the *etype-id* argument to the hexadecimal value 800, 809b, or 86dd. The hexadecimal values 800, 809b, and 86dd correspond to IPv4, AppleTalk, and IPv6, respectively.

Examples

Assign ARP packets in Ethernet II encapsulation and IPv4 packets to VLAN 3 for transmission. (The protocol type ID for ARP is 0806 in hexadecimal notation.)

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] protocol-vlan 1 ipv4
[Sysname-vlan3] protocol-vlan 2 mode ethernetii etype 0806
```

Related commands

display protocol-vlan interface

display protocol-vlan vlan

port protocol-vlan

VLAN group commands

display vlan-group

Use **display vlan-group** to display VLAN group information.

Syntax

display vlan-group [*group-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group-name: Specifies a VLAN group by its name, a case-sensitive string of 1 to 31 characters. The first character must be an alphabetical character. If you do not specify this argument, the command displays information about all VLAN groups.

Examples

Display information about VLAN group **test001**.

```
<Sysname> display vlan-group test001
VLAN group: test001
```

```
     VLAN list: 2-4 100 200
```

Display information about all VLAN groups.

```
<Sysname> display vlan-group
VLAN group: test001
     VLAN list: 2-4 100 200
VLAN group: rnd
     VLAN list: Null
```

Table 10 Command output

Field	Description
VLAN group	Name of the VLAN group.
VLAN list	VLAN list in the VLAN group.

Related commands

vlan-group

vlan-list

vlan-group

Use **vlan-group** to create a VLAN group and enter its view, or enter the view of an existing VLAN group.

Use **undo vlan-group** to delete a VLAN group.

Syntax

vlan-group *group-name*

undo vlan-group *group-name*

Default

No VLAN groups exist.

Views

System view

Predefined user roles

network-admin

Parameters

group-name: Specifies a VLAN group by its name, a case-sensitive string of 1 to 31 characters. The first character must be an alphabetical character.

Usage guidelines

A VLAN group includes a set of VLANs. You can add multiple VLAN lists to a VLAN group.

Examples

Create a VLAN group named **test001** and enter VLAN group view.

```
<Sysname> system-view
[Sysname] vlan-group test001
[Sysname-vlan-group-test001]
```

Related commands

vlan-list

vlan-list

Use **vlan-list** to add VLANs to a VLAN group.

Use **undo vlan-list** to remove VLANs from a VLAN group.

Syntax

vlan-list *vlan-id-list*

undo vlan-list *vlan-id-list*

Default

No VLANs exist in a VLAN group.

Views

VLAN group view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN ID or a range of VLAN IDs in the form of *vlan-id1* **to** *vlan-id2*. The value range for VLAN IDs is 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument.

Examples

Add VLAN 2 through VLAN 4, VLAN 100, and VLAN 200 to VLAN group **test001**.

```
<Sysname> system-view
[Sysname] vlan-group test001
[Sysname-vlan-group-test001] vlan-list 2 to 4 100 200
```

Related commands

vlan-group

Private VLAN commands

S5110V2-SI, S5000V3-EI, S5000V5-EI, S5000E-X, S5000X-EI, WAS6000 switches do not support private VLAN.

display private-vlan

Use **display private-vlan** to display information about primary VLANs and their associated secondary VLANs.

Syntax

display private-vlan [*primary-vlan-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

primary-vlan-id: Specifies a primary VLAN ID in the range of 1 to 4094. If you do not specify a primary VLAN ID, this command displays information about all primary VLANs and their associated secondary VLANs.

Examples

Display information about primary VLANs and their associated secondary VLANs.

```
<Sysname> display private-vlan
 Primary VLAN ID: 2
 Secondary VLAN ID: 3-4

 VLAN ID: 2
 VLAN type: Static
 Private VLAN type: Primary
 Route interface: Configured
 IPv4 address: 1.1.1.1
 IPv4 subnet mask: 255.255.255.0
 IPv6 global unicast addresses:
   2001::1, subnet is 2001::/64 [TENTATIVE]
 Description: VLAN 0002
 Name: VLAN 0002
 Tagged ports:   None
 Untagged ports:
    GigabitEthernet1/0/2
    GigabitEthernet1/0/3
    GigabitEthernet1/0/4

 VLAN ID: 3
 VLAN type: Static
 Private VLAN type: Secondary
```

```
Route interface: Not configured
Description: VLAN 0003
Name: VLAN 0003
Tagged ports:   None
Untagged ports:
   GigabitEthernet1/0/2
   GigabitEthernet1/0/3

VLAN ID: 4
VLAN type: Static
Private VLAN type: Secondary
Route interface: Not configured
Description: VLAN 0004
Name: VLAN 0004
Tagged ports:   None
Untagged ports:
   GigabitEthernet1/0/2
   GigabitEthernet1/0/4
```

Table 11 Command output

Field	Description
VLAN type	VLAN type, dynamic or static.
Private VLAN type	Private VLAN type: • **Primary**—Primary VLAN. • **Secondary**—Secondary VLAN. • **Isolated secondary**—Secondary VLAN configured with port isolation at Layer 2.
Route interface	Whether a VLAN interface is created for the VLAN: • Configured. • Not configured.
IPv4 address	Primary IPv4 address of the VLAN interface. This field is displayed only when an IPv4 address is configured for the VLAN interface. When the VLAN interface is also configured with secondary IPv4 addresses, you can view them by using one of the following commands: • **`display interface vlan-interface`**. • **`display this`** (VLAN interface view).
IPv4 subnet mask	Subnet mask for the primary IPv4 address of the VLAN interface. This field is displayed only when an IPv4 address is configured for the VLAN interface.
IPv6 global unicast addresses	Global unicast IPv6 address of the VLAN interface. This field is not displayed when no IPv6 address is configured for the VLAN interface. The IPv6 address states are as follows: • **TENTATIVE**—Initial state. DAD is being performed or is to be performed on the address. An address in this state cannot be used as the source address or destination address of packets. • **DUPLICATE**—DAD has been completed for the address. The address is not unique on the link and cannot be used. • **PREFERRED**—The address is preferred and can be used as the source or destination address of a packet. If an address is in this state, the command does not display the address state.

Field	Description
	• **DEPRECATED**—The address is beyond the preferred lifetime but within the valid lifetime. It is valid, but it cannot be used as the source address for a new connection. Packets destined to the address are processed correctly.
Description	VLAN description.
Name	VLAN name.
Tagged ports	Tagged members of the VLAN.
Untagged ports	Untagged members of the VLAN.

Related commands

`private-vlan` (VLAN view)

`private-vlan primary`

port private-vlan host

Use **`port private-vlan host`** to configure a port as a host port.

Use **`undo port private-vlan`** to restore the default.

Syntax

`port private-vlan host`

`undo port private-vlan`

Default

A port is not a host port.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

If the port has been assigned to a secondary VLAN, the command assigns the port to the primary VLAN associated with the secondary VLAN. Also, the following events occur:

- For an access port, the device performs the following operations:
  - Changes the port link type to hybrid.
  - Configures the secondary VLAN as the PVID.
  - Assigns the port to the primary VLAN as an untagged member.
- For a trunk port, the device does not change the port link type or PVID.
- For a hybrid port, the device does not change the port link type or PVID.
  - If the hybrid port has been a tagged or untagged member of the primary VLAN, this member attribute remains in the primary VLAN.
  - If the hybrid port does not allow the primary VLAN, the device assigns the port to the primary VLAN as an untagged member.

You can assign the port to a secondary VLAN before or after you execute this command.

The **undo port private-vlan** command does not change the VLAN attributes (allowed VLANs, port link type, and PVID) of the port.

The **port private-vlan host** command is mutually exclusive with the **port private-vlan trunk promiscuous** and **port private-vlan trunk secondary** commands.

Examples

In this example, VLAN 20 is a secondary VLAN and is associated with primary VLAN 2.

Configure GigabitEthernet 1/0/1 as a host port, and then verify the configuration.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port private-vlan host
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port private-vlan host
#
return
```

The output show that GigabitEthernet 1/0/1 is operating in bridge mode and is a host port.

Assign GigabitEthernet 1/0/1 to VLAN 20, and then verify the configuration.

```
[Sysname-GigabitEthernet1/0/1] port access vlan 20
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port private-vlan host
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 2 20 untagged
 port hybrid pvid vlan 20
#
return
```

The output shows that:

- GigabitEthernet 1/0/1 is an untagged member of secondary VLAN 20 and primary VLAN 2.
- The port link type of GigabitEthernet 1/0/1 is hybrid and its PVID is VLAN 20.

Related commands

port private-vlan promiscuous

port private-vlan trunk promiscuous

port private-vlan trunk secondary

private-vlan (VLAN view)

private-vlan primary

port private-vlan promiscuous

Use **port private-vlan promiscuous** to configure a port as a promiscuous port of the specified VLAN and assign the port to the VLAN.

Use **undo port private-vlan** to restore the default.

Syntax

port private-vlan *vlan-id* **promiscuous**

undo port private-vlan

Default

A port is not a promiscuous port of any VLANs.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies a VLAN ID in the range of 1 to 4094. Though VLAN 1 is in the valid value range, it cannot be configured in the command.

Usage guidelines

If the specified VLAN is a primary VLAN that has been associated with secondary VLANs, the command assigns the port to the associated secondary VLANs. Also, the following events occur:

- For an access port, the device performs the following operations:
  - Changes the port link type to hybrid.
  - Configures the primary VLAN as the PVID.
  - Assigns the port to the primary VLAN and its associated secondary VLANs as an untagged member.
- For a trunk port, the device does not change the port link type or PVID.
- For a hybrid port, the device does not change the port link type or PVID.
  - If the hybrid port has been a tagged or untagged member of the primary VLAN and part of its associated secondary VLANs, this member attribute remains in these VLANs. The device assigns the hybrid port to the rest of the associated secondary VLANs as an untagged member.
  - If the hybrid port does not allow any of the primary VLAN and its associated secondary VLANs, the command assigns the port to these VLANs as an untagged member.

If you execute this command on a promiscuous port multiple times, the most recent configuration takes effect.

The **undo port private-vlan** command does not change the VLAN attributes (allowed secondary VLANs, link type, and PVID) of the port. When you execute the **undo port private-vlan** command on a promiscuous port of a VLAN, the command removes the port from the VLAN.

You can configure the VLAN as a primary VLAN before or after you execute the **port private-vlan promiscuous** command.

This command is mutually exclusive with the **port private-vlan trunk promiscuous** and **port private-vlan trunk secondary** commands.

Examples

In this example, VLAN 2 is a primary VLAN, and it is associated with secondary VLAN 20.

Display information about GigabitEthernet 1/0/1.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
#
return
```

Configure GigabitEthernet 1/0/1 as a promiscuous port of VLAN 2, and then verify the configuration.

```
[Sysname-GigabitEthernet1/0/1] port private-vlan 2 promiscuous
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 port private-vlan 2 promiscuous
 undo port hybrid vlan 1
 port hybrid vlan 2 20 untagged
 port hybrid pvid vlan 2
#
return
```

The output shows that:

- GigabitEthernet 1/0/1 is a promiscuous port of VLAN 2.
- GigabitEthernet 1/0/1 is an untagged member of primary VLAN 2 and secondary VLAN 20.
- The port link type of GigabitEthernet 1/0/1 is hybrid and its PVID is VLAN 2.

Execute the **undo port private-vlan** command on GigabitEthernet 1/0/1, and then verify the configuration.

```
[Sysname-GigabitEthernet1/0/1] undo port private-vlan
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 20 untagged
 port hybrid pvid vlan 2
#
return
```

The output shows that:

- GigabitEthernet 1/0/1 is removed from primary VLAN 2.
- GigabitEthernet 1/0/1 is an untagged member of VLAN 20.
- The link type and PVID of GigabitEthernet 1/0/1 do not change.

Related commands

port private-vlan host

port private-vlan trunk promiscuous

port private-vlan trunk secondary

private-vlan (VLAN view)

private-vlan primary

port private-vlan trunk promiscuous

Use **port private-vlan trunk promiscuous** to configure a port as a trunk promiscuous port of the specified VLANs and assign the port to these VLANs.

Use **undo port private-vlan trunk promiscuous** to cancel the trunk promiscuous attribute of a port in the specified VLANs.

Syntax

port private-vlan *vlan-id-list* **trunk promiscuous**

undo port private-vlan *vlan-id-list* **trunk promiscuous**

Default

A port is not a trunk promiscuous port of any VLANs.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 primary VLAN items. Each item specifies a primary VLAN ID or a range of primary VLAN IDs in the form of *vlan-id1* **to** *vlan-id2*. The value range for primary VLAN IDs is 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument. Though the system default VLAN (VLAN 1) is in the valid value range, it cannot be configured in the command.

Usage guidelines

If the specified VLANs are primary VLANs that have been associated with secondary VLANs, the command assigns the port to the associated secondary VLANs. Also, the following events occur:

- For an access port, the device performs the following operations:
  - Changes the port link type to hybrid. The PVID of the port does not change.
  - Assigns the port to the primary VLANs and the associated secondary VLANs as a tagged member.
- For a trunk port, the device does not change the port link type or PVID.
- For a hybrid port, the device does not change the port link type or PVID.
  - If the hybrid port has been a tagged or untagged member of part of the primary VLANs and their associated secondary VLANs, this member attribute remains in these VLANs. The device assigns the hybrid port to the rest of the primary VLANs and their associated secondary VLANs as a tagged member.
  - If the hybrid port does not allow any of the primary VLANs and their associated secondary VLANs, the device assigns the port to these VLANs as a tagged member.

The **undo** form of this command does not change the VLAN attributes (allowed secondary VLANs, port link type, and PVID) of the port.

If you execute the **undo** form of this command on a trunk promiscuous port, the command removes the port from the VLANs specified by the *vlan-id-list* argument.

You can configure the specified VLANs as primary VLANs before or after you execute this command.

This command is mutually exclusive with the **port private-vlan host**, **port private-vlan promiscuous** and **port private-vlan trunk secondary** commands.

For an uplink port to permit multiple primary VLANs, use the **port private-vlan trunk promiscuous** command to assign the port to these VLANs. The port can then transmit packets from these primary VLANs with VLAN tags. For an uplink port to permit only one primary VLAN, use the **port private-vlan promiscuous** command to assign the port to the VLAN. The port can then transmit packets from the primary VLAN without VLAN tags.

Examples

In this example, VLANs 2 and 3 are primary VLANs. VLAN 2 is associated with secondary VLAN 20. VLAN 3 is associated with secondary VLAN 30.

Display information about GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
#
return
```

Configure GigabitEthernet 1/0/1 as a trunk promiscuous port of VLANs 2 and 3, and then verify the configuration.

```
[Sysname-GigabitEthernet1/0/1] port private-vlan 2 3 trunk promiscuous
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 port private-vlan 2 3 trunk promiscuous
 port hybrid vlan 2 3 20 30 tagged
 port hybrid vlan 1 untagged
#
return
```

The output shows that:

- GigabitEthernet 1/0/1 is a trunk promiscuous port of VLANs 2 and 3.
- GigabitEthernet1/0/1 is a tagged member of VLANs 2, 3, 20, and 30.
- The port link type of GigabitEthernet 1/0/1 is hybrid.

Execute the **undo port private-vlan trunk promiscuous** command on GigabitEthernet 1/0/1, and then verify the configuration.

```
[Sysname-GigabitEthernet1/0/1] undo port private-vlan 2 3 trunk promiscuous
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 20 30 tagged
 port hybrid vlan 1 untagged
```

```
#
return
```

The output shows that:

- GigabitEthernet 1/0/1 is removed from VLANs 2 and 3.
- GigabitEthernet 1/0/1 is a tagged member of VLANs 20 and 30.
- The port link type and PVID of GigabitEthernet 1/0/1 do not change.

Related commands

port private-vlan host

port private-vlan promiscuous

port private-vlan trunk secondary

private-vlan (VLAN view)

private-vlan primary

port private-vlan trunk secondary

Use **port private-vlan trunk secondary** to configure a port as a trunk secondary port of the specified VLANs and assign the port to these VLANs.

Use **undo port private-vlan trunk secondary** to cancel the trunk secondary attribute of a port in the specified VLANs.

Syntax

port private-vlan *vlan-id-list* **trunk secondary**

undo port private-vlan *vlan-id-list* **trunk secondary**

Default

A port is not a trunk secondary port of any VLANs.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 secondary VLAN items. Each item specifies a secondary VLAN ID or a range of secondary VLAN IDs in the form of *vlan-id1* **to** *vlan-id2*. The value range for secondary VLAN IDs is 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument. Though the system default VLAN (VLAN 1) is in the valid value range, it cannot be configured in the command.

Usage guidelines

If the specified VLANs are secondary VLANs that have been associated with primary VLANs, the command also assigns the port to the associated primary VLANs. Also, the following events occur:

- For an access port, the device performs the following operations:
  - Changes the port link type to hybrid. The PVID of the port does not change.
  - Assigns the port to the secondary VLANs and the associated primary VLANs as a tagged member.

- For a trunk port, the device does not change the port link type or PVID.
- For a hybrid port, the device does not change the port link type or PVID.
  - If the port has been an untagged or tagged member of part of the secondary VLANs and their associated primary VLANs, this member attribute remains in these VLANs. The device assigns the port to the rest of the secondary VLANs and their associated primary VLANs as a tagged member.
  - If the hybrid port does not allow any of the secondary VLANs and their associated primary VLANs, the device assigns the port to these VLANs as a tagged member.

A trunk secondary port can join only one secondary VLAN among all secondary VLANs associated with a primary VLAN. However, it can join multiple secondary VLANs that are associated with different primary VLANs.

The **undo** form of this command does not change the VLAN attributes (allowed primary VLANs, port link type, and PVID) of the port.

When you execute the **undo** form of this command on a trunk secondary port of the VLANs specified by the *vlan-id-list* argument, one of the following events occurs:

- If the port is an access port, the device does not change the VLAN configuration of the port.
- If the port is a trunk or hybrid port, the device removes the port from the specified VLANs.

You can associate the specified VLANs with their respective primary VLANs before or after you execute this command.

This command does not take effect on the specified VLAN if any of the following conditions applies:

- The specified VLAN does not exist.
- The specified VLAN is not a secondary VLAN and is used for other purposes.
- The specified VLAN shares the same primary VLAN with other secondary VLANs, and the current port has been configured as a trunk secondary port in one of the other secondary VLANs.

This command is mutually exclusive with the **port private-vlan host**, **port private-vlan promiscuous** and **port private-vlan trunk promiscuous** commands.

For a downlink port to permit multiple secondary VLANs associated with different primary VLANs, use the **port private-vlan trunk secondary** command to assign the port to these secondary VLANs. The port can then transmit packets from these secondary VLANs with VLAN tags. For a downlink port to permit only one secondary VLAN, use the **port private-vlan host** command to assign the port to the secondary VLAN. The port can then transmit packets from the secondary VLAN without VLAN tags.

Examples

- In this example, VLANs 2 and 3 are primary VLANs. VLAN 2 is associated with secondary VLAN 20. VLAN 3 is associated with secondary VLAN 30.

  # Display information about GigabitEthernet 1/0/1.

  ```
  <Sysname> system-view
  [Sysname] interface gigabitethernet 1/0/1
  [Sysname-GigabitEthernet1/0/1] display this
  #
  interface GigabitEthernet1/0/1
   port link-mode bridge
  #
  return
  ```

  # Configure GigabitEthernet 1/0/1 as a trunk secondary port of VLANs 20 and 30, and then verify the configuration.

  ```
  [Sysname-GigabitEthernet1/0/1] port private-vlan 20 30 trunk secondary
  ```

```
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 2 3 20 30 tagged
 port hybrid vlan 1 untagged
 port private-vlan 20 30 trunk secondary
#
return
```

The output shows that:

- GigabitEthernet 1/0/1 is a trunk secondary port of VLANs 20 and 30.
- GigabitEthernet 1/0/1 is a tagged member of VLANs 2, 3, 20, and 30.
- The port link type of GigabitEthernet 1/0/1 is hybrid.

Execute the **undo port private-vlan trunk secondary** command on GigabitEthernet 1/0/1, and then verify the configuration.

```
[Sysname-GigabitEthernet1/0/1] undo port private-vlan 20 30 trunk secondary
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 2 3 tagged
 port hybrid vlan 1 untagged
#
return
```

The output shows that:

- GigabitEthernet 1/0/1 is removed from VLANs 20 and 30.
- GigabitEthernet 1/0/1 is a tagged member of VLANs 2 and 3.
- The port link type and PVID of GigabitEthernet 1/0/1 do not change.

- In this example, VLAN 10 is not a secondary VLAN.

  # Display information about GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
#
return
```

  # Configure GigabitEthernet 1/0/1 as a trunk secondary port of VLAN 10, and then verify the configuration.

```
[Sysname-GigabitEthernet1/0/1] port private-vlan 10 trunk secondary
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
```

```
 port link-type hybrid
 port hybrid vlan 10 tagged
 port hybrid vlan 1 untagged
 port private-vlan 10 trunk secondary
#
return
```

The output shows that:

- GigabitEthernet 1/0/1 is a trunk secondary port of VLAN 10.
- GigabitEthernet 1/0/1 is a tagged member of VLAN 10.
- The port link type of GigabitEthernet 1/0/1 is hybrid.

Execute the **undo port private-vlan trunk secondary** command on GigabitEthernet1/0/1, and then verify the configuration.

```
[Sysname-GigabitEthernet1/0/1] undo port private-vlan 10 trunk secondary
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 1 untagged
#
return
```

The output shows that:

- GigabitEthernet 1/0/1 is removed from VLAN 10.
- The port link type and PVID of GigabitEthernet 1/0/1 do not change.

Related commands

port private-vlan host

port private-vlan promiscuous

port private-vlan trunk promiscuous

private-vlan (VLAN view)

private-vlan isolated

private-vlan primary

private-vlan (VLAN interface view)

Use **private-vlan secondary** to enable Layer 3 communication between secondary VLANs that are associated with a primary VLAN.

Use **undo private-vlan** to cancel the Layer 3 communication configuration for secondary VLANs that are associated with a primary VLAN.

Syntax

private-vlan secondary *vlan-id-list*

undo private-vlan [**secondary** *vlan-id-list*]

Default

Secondary VLANs are isolated at Layer 3.

Views

VLAN interface view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 secondary VLAN items. Each item specifies a secondary VLAN ID or a range of secondary VLAN IDs in the form of *vlan-id1* **to** *vlan-id2*. The value range for secondary VLAN IDs is 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument.

Usage guidelines

This command takes effect only when the following conditions exist:

- This command is executed in VLAN interface view of the primary VLAN interface.
- Secondary VLANs are associated with the primary VLAN.
- No VLAN interfaces are created for secondary VLANs.
- An IP address is assigned to the primary VLAN interface.
- Local proxy ARP or ND is enabled on the primary VLAN interface.

You can create VLAN interfaces for secondary VLANs that are not enabled with Layer 3 communication. If secondary VLANs are enabled with Layer 3 communication, do not create VLAN interfaces for them.

When you execute this command in the same primary VLAN interface view multiple times, all the specified secondary VLANs are interoperable at Layer 3.

When you execute the **undo private-vlan** command, follow these guidelines:

- If you specify the **secondary** *vlan-id-list* option, this command cancels the Layer 3 communication configuration only for the specified secondary VLANs.
- If you do not specify the **secondary** *vlan-id-list* option, this command cancels the Layer 3 communication configuration for all secondary VLANs of the primary VLAN.

Examples

This example shows how to meet the following requirements:

- VLAN 4 is a secondary VLAN, and it is associated with primary VLAN 2.
- The uplink port (GigabitEthernet 1/0/2) is a promiscuous port of VLAN 2.
- Downlink ports GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 are host ports of VLANs 3 and 4, respectively.
- Secondary VLANs 3 and 4 can communicate at Layer 3.

Configure VLAN 2 as a primary VLAN and associate it with secondary VLANs 3 and 4.

```
<Sysname> system-view
[Sysname] vlan 3 to 4
[Sysname] vlan 2
[Sysname-vlan2] private-vlan primary
[Sysname-vlan2] private-vlan secondary 3 to 4
[Sysname-vlan2] quit
```

Configure the uplink port (GigabitEthernet 1/0/2) as a promiscuous port of VLAN 2.

```
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] port private-vlan 2 promiscuous
[Sysname-GigabitEthernet1/0/2] quit
```

Assign downlink port GigabitEthernet 1/0/3 to VLAN 3 and configure the port as a host port.

```
[Sysname] interface gigabitethernet 1/0/3
[Sysname-GigabitEthernet1/0/3] port access vlan 3
[Sysname-GigabitEthernet1/0/3] port private-vlan host
[Sysname-GigabitEthernet1/0/3] quit
```

Assign downlink port GigabitEthernet 1/0/4 to VLAN 4 and configure the port as a host port.

```
[Sysname] interface gigabitethernet 1/0/4
[Sysname-GigabitEthernet1/0/4] port access vlan 4
[Sysname-GigabitEthernet1/0/4] port private-vlan host
[Sysname-GigabitEthernet1/0/4] quit
```

Create VLAN-interface 2 and enable Layer 3 communication between secondary VLANs 3 and 4.

```
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] private-vlan secondary 3 to 4
```

Assign an IP address to VLAN-interface 2.

```
[Sysname-Vlan-interface2] ip address 192.168.1.1 255.255.255.0
```

Enable local proxy ARP on VLAN-interface 2.

```
[Sysname-Vlan-interface2] local-proxy-arp enable
```

Related commands

private-vlan (VLAN view)

private-vlan primary

private-vlan (VLAN view)

Use **private-vlan** to associate a primary VLAN with the specified secondary VLANs.

Use **undo private-vlan** to dissociate a primary VLAN from the specified secondary VLANs.

Syntax

private-vlan secondary *vlan-id-list*

undo private-vlan [**secondary** *vlan-id-list*]

Default

A primary VLAN is not associated with any secondary VLANs.

Views

VLAN view

Predefined user roles

network-admin

Parameters

secondary *vlan-id-list*: Specifies a space-separated list of up to 10 secondary VLAN items. Each item specifies a secondary VLAN ID or a range of secondary VLAN IDs in the form of *vlan-id1* **to** *vlan-id2*. The value range for secondary VLAN IDs is 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument. Though the system default VLAN (VLAN 1) is in the valid value range, it cannot be configured in the command.

Usage guidelines

A primary VLAN can be associated with multiple secondary VLANs. When you execute this command in the same VLAN view multiple times, all the specified secondary VLANs are associated with the primary VLAN.

The configuration synchronization is triggered based on the interface configuration when the following conditions exist:

- This command is configured for a primary VLAN.
- Ports on the device are promiscuous, trunk promiscuous, or host ports.

When you execute the **undo private-vlan** command, follow these guidelines:

- If you specify the **secondary** *vlan-id-list* option, this command dissociates the primary VLAN from the specified secondary VLANs.
- If you do not specify the **secondary** *vlan-id-list* option, this command dissociates the primary VLAN from all secondary VLANs.

Examples

Associate primary VLAN 2 with secondary VLANs 3 and 4.

```
<Sysname> system-view
[Sysname] vlan 3 to 4
[Sysname] vlan 2
[Sysname-vlan2] private-vlan primary
[Sysname-vlan2] private-vlan secondary 3 to 4
```

Related commands

port private-vlan host

port private-vlan promiscuous

port private-vlan trunk promiscuous

port private-vlan trunk secondary

primary-vlan primary

private-vlan community

Use **private-vlan community** to enable Layer 2 communication between ports in a secondary VLAN.

Syntax

private-vlan community

Default

Ports in the same secondary VLAN can communicate with each other at Layer 2.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

This command and the **undo private-vlan isolated** command have the same function.

When you use the **save** command to save the configuration, the **private-vlan community** command is not saved into the configuration file.

Examples

This example shows how to meet the following requirements:

- VLAN 4 is a secondary VLAN, and it is associated with primary VLAN 2.
- GigabitEthernet 1/0/1 is a promiscuous port of VLAN 2.
- GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 are host ports.
- GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 can communicate at Layer 2 in secondary VLAN 4.

Configure VLAN 2 as a primary VLAN and associate it with secondary VLAN 4.

```
<Sysname> system-view
[Sysname] vlan 4
[Sysname-vlan4] quit
[Sysname] vlan 2
[Sysname-vlan2] private-vlan primary
[Sysname-vlan2] private-vlan secondary 4
[Sysname-vlan2] quit
```

Configure GigabitEthernet 1/0/1 as a promiscuous port of VLAN 2.

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port private-vlan 2 promiscuous
[Sysname-GigabitEthernet1/0/1] quit
```

Assign GigabitEthernet 1/0/2 to VLAN 4 and configure the port as a host port.

```
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] port access vlan 4
[Sysname-GigabitEthernet1/0/2] port private-vlan host
[Sysname-GigabitEthernet1/0/2] quit
```

Assign GigabitEthernet 1/0/3 to VLAN 4 and configure the port as a host port.

```
[Sysname] interface gigabitethernet 1/0/3
[Sysname-GigabitEthernet1/0/3] port access vlan 4
[Sysname-GigabitEthernet1/0/3] port private-vlan host
[Sysname-GigabitEthernet1/0/3] quit
```

Enable Layer 2 communication in secondary VLAN 4.

```
[Sysname] vlan 4
[Sysname-vlan4] private-vlan community
```

Related commands

`private-vlan isolated`

private-vlan isolated

Use **`private-vlan isolated`** to isolate ports in a secondary VLAN at Layer 2.

Use **`undo private-vlan isolated`** to restore the default.

Syntax

`private-vlan isolated`

`undo private-vlan isolated`

Default

Ports in the same secondary VLAN can communicate with each other at Layer 2.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

This command takes effect when the following conditions exist:

- The secondary VLAN is associated with a primary VLAN.
- The ports are configured as host ports or trunk secondary ports of the secondary VLAN.

This command is mutually exclusive with the primary VLAN configuration commands.

Examples

This example shows how to meet the following requirements:

- VLAN 4 is a secondary VLAN, and it is associated with primary VLAN 2.
- GigabitEthernet 1/0/1 is a promiscuous port of VLAN 2.
- GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 are host ports.
- GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 are isolated at Layer 2 in secondary VLAN 4.

Configure VLAN 2 as a primary VLAN and associate it with secondary VLAN 4.

```
<Sysname> system-view
[Sysname] vlan 4
[Sysname-vlan4] quit
[Sysname] vlan 2
[Sysname-vlan2] private-vlan primary
[Sysname-vlan2] private-vlan secondary 4
[Sysname-vlan2] quit
```

Configure GigabitEthernet 1/0/1 as a promiscuous port of VLAN 2.

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port private-vlan 2 promiscuous
[Sysname-GigabitEthernet1/0/1] quit
```

Assign GigabitEthernet 1/0/2 to VLAN 4 and configure the port as a host port.

```
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] port access vlan 4
[Sysname-GigabitEthernet1/0/2] quit
[Sysname-GigabitEthernet1/0/2] port private-vlan host
```

Assign GigabitEthernet 1/0/3 to VLAN 4 and configure the port as a host port.

```
[Sysname] interface gigabitethernet 1/0/3
[Sysname-GigabitEthernet1/0/3] port access vlan 4
[Sysname-GigabitEthernet1/0/3] port private-vlan host
```

Configure port isolation at Layer 2 in secondary VLAN 4.

```
[Sysname] vlan 4
[Sysname-vlan4] private-vlan isolated
```

Related commands

private-vlan (VLAN view)

private-vlan community

private-vlan primary

private-vlan primary

Use **private-vlan primary** to configure a VLAN as a primary VLAN.

Use **undo private-vlan primary** to restore the default.

Syntax

private-vlan primary

undo private-vlan primary

Default

A VLAN is not a primary VLAN.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

The configuration synchronization is triggered based on the interface configuration when the following conditions exist:

- This command is configured for a VLAN that has been associated with secondary VLANs.
- Ports on the device are promiscuous, trunk promiscuous, host, or trunk secondary ports.

Examples

Configure VLAN 5 as a primary VLAN.

```
<Sysname> system-view
[Sysname] vlan 5
[Sysname-vlan5] private-vlan primary
```

Related commands

port private-vlan host

port private-vlan promiscuous

port private-vlan trunk promiscuous

port private-vlan trunk secondary

private-vlan primary

Voice VLAN commands

S5110V2-SI, S5000V3-EI, S5000V5-EI, S5000E-X, S5000X-EI, WAS6000 switches do not support voice VLAN.

display voice-vlan mac-address

Use **display voice-vlan mac-address** to display the OUI addresses supported on the device.

Syntax

display voice-vlan mac-address

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the OUI addresses supported on the device.

```
<Sysname> display voice-vlan mac-address
OUI Address     Mask            Description
0001-e300-0000  ffff-ff00-0000  Siemens phone
0003-6b00-0000  ffff-ff00-0000  Cisco phone
0004-0d00-0000  ffff-ff00-0000  Avaya phone
000f-e200-0000  ffff-ff00-0000  H3C Aolynk phone
0060-b900-0000  ffff-ff00-0000  Philips/NEC phone
00d0-1e00-0000  ffff-ff00-0000  Pingtel phone
00e0-7500-0000  ffff-ff00-0000  Polycom phone
00e0-bb00-0000  ffff-ff00-0000  3Com phone
```

Table 12 Command output

Field	Description
OUI Address	OUI address allowed on the device.
Mask	Mask of the OUI address.
Description	Description of the OUI address.

Related commands

voice-vlan mac-address

display voice-vlan state

Use **display voice-vlan state** to display voice VLAN information.

Syntax

display voice-vlan state

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display voice VLAN information.

```
<Sysname> display voice-vlan state
 Current voice VLANs: 1
 Voice VLAN security mode: Security
 Voice VLAN aging time: 1440 minutes
 Voice VLAN enabled ports and their modes:
 Port                      VLAN        Mode        CoS         DSCP
 GE1/0/1                   111         Auto        6           46
```

Table 13 Command output

Field	Description
Current Voice VLANs	Number of existing voice VLANs.
Voice VLAN security mode	Voice VLAN mode: • Security. • Normal.
Voice VLAN aging time	Voice VLAN aging timer. **No aging** indicates that the voice VLAN does not age out.
Voice VLAN enabled ports and their modes	Voice VLAN-enabled ports and their voice VLAN assignment modes.
Port	Name of the voice VLAN-enabled port.
VLAN	ID of the voice VLAN enabled on the port.
Mode	Voice VLAN assignment mode of the port: • Manual. • Automatic.

Related commands

voice-vlan aging

voice-vlan enable

voice-vlan mode auto

voice-vlan security enable

voice-vlan aging

Use **voice-vlan aging** to set the voice VLAN aging timer.

Use **undo voice-vlan aging** to restore the default.

Syntax

voice-vlan aging *minutes*

undo voice-vlan aging

Default

The voice VLAN aging timer is 1440 minutes (24 hours).

Views

System view

Predefined user roles

network-admin

Parameters

minutes: Sets the voice VLAN aging timer to 0 minutes or a value in the range of 5 to 43200 minutes. If you set the voice VLAN aging timer to 0 minutes, the voice VLAN does not age out.

Usage guidelines

In automatic voice VLAN assignment mode, after a port is assigned to a voice VLAN, the voice VLAN is controlled by a voice VLAN aging timer. The voice VLAN aging timer starts only when the dynamic MAC address entry of the voice VLAN ages out. If no voice packets are received on the port before the voice VLAN aging timer expires, the device removes the port from the voice VLAN.

The aging period for a voice VLAN equals the sum of the voice VLAN aging timer and the aging timer for its dynamic MAC address entry. For more information about the aging timer for dynamic MAC address entries, see MAC address table configuration in *Layer 2—LAN Switching Configuration Guide*.

Set the voice VLAN aging timer only when the voice VLAN assignment mode is automatic.

Examples

Set the voice VLAN aging timer to 100 minutes.

```
<Sysname> system-view
[Sysname] voice-vlan aging 100
```

Related commands

display voice-vlan state

voice-vlan enable

Use **voice-vlan enable** to enable the voice VLAN feature on a port.

Use **undo voice-vlan enable** to disable the voice VLAN feature on a port.

Syntax

voice-vlan *vlan-id* **enable**

undo voice-vlan [*vlan-id*] **enable**

Default

The voice VLAN feature is disabled on ports.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies a voice VLAN ID in the range of 2 to 4094.

Usage guidelines

Use this command only on a hybrid or trunk port operating in automatic voice VLAN assignment mode.

Before you execute this command, make sure the specified VLAN already exists.

Examples

Enable the voice VLAN feature on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] voice-vlan 2 enable
```

Related commands

display voice-vlan state

voice-vlan mode auto

voice-vlan mac-address

Use **voice-vlan mac-address** to configure the OUI address information for voice packet identification.

Use **undo voice-vlan mac-address** to delete an OUI address.

Syntax

voice-vlan mac-address *mac-address* **mask** *oui-mask* [**description** *text*]

undo voice-vlan mac-address *oui*

Default

System default OUI addresses exist.

Table 14 System default OUI addresses

Number	OUI address	Vendor
1	0001-e300-0000	Siemens phone
2	0003-6b00-0000	Cisco phone
3	0004-0d00-0000	Avaya phone
4	000f-e200-0000	H3C Aolynk phone
5	0060-b900-0000	Philips/NEC phone
6	00d0-1e00-0000	Pingtel phone
7	00e0-7500-0000	Polycom phone
8	00e0-bb00-0000	3Com phone

Views

System view

Predefined user roles

network-admin

Parameters

mac-address: Specifies a source MAC address of voice traffic, in the format of H-H-H. For example, 1234-1234-1234.

mask *oui-mask*: Specifies the valid length of the OUI address by using a mask in the format of H-H-H. The mask contains consecutive 1s and 0s. For example, ffff-0000-0000. To match the voice devices of a vendor, set the mask to ffff-ff00-0000.

description *text*: Specifies the OUI address description, a case-sensitive string of 1 to 30 characters.

oui: Specifies an OUI address to delete, in the format of H-H-H. For example, 1234-1200-0000. An OUI address is the logical AND result of the *mac-address* and *oui-mask* arguments. It cannot be a broadcast address, a multicast address, or an all-zero address.

Usage guidelines

You can manually delete or add the system default OUI addresses.

The device supports a maximum of 128 OUI addresses.

Examples

Add OUI address **1234-1200-0000** by specifying the MAC address as 1234-1234-1234 and the mask as fff-ff00-0000. Configure the OUI address description as **PhoneA**.

```
<Sysname> system-view
[Sysname] voice-vlan mac-address 1234-1234-1234 mask ffff-ff00-0000 description PhoneA
```

Related commands

display voice-vlan mac-address

voice-vlan mode auto

Use **voice-vlan mode auto** to configure a port to operate in automatic voice VLAN assignment mode.

Use **undo voice-vlan mode auto** to configure a port to operate in manual voice VLAN assignment mode.

Syntax

voice-vlan mode auto

undo voice-vlan mode auto

Default

A port operates in automatic voice VLAN assignment mode.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

To make a voice VLAN take effect on a port operating in manual mode, you must manually assign the port to the voice VLAN.

Examples

Configure GigabitEthernet 1/0/1 to operate in manual voice VLAN assignment mode.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo voice-vlan mode auto
```

Related commands

display voice-vlan state

voice-vlan security enable

Use **voice-vlan security enable** to enable the voice VLAN security mode.

Use **undo voice-vlan security enable** to disable the voice VLAN security mode.

Syntax

voice-vlan security enable

undo voice-vlan security enable

Default

The voice VLAN security mode is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

In security mode, a voice VLAN transmits only voice packets whose source MAC addresses match the OUI addresses of the device.

In normal mode, a voice VLAN transmits voice packets and non-voice packets.

Examples

Disable the voice VLAN security mode.

```
<Sysname> system-view
[Sysname] undo voice-vlan security enable
```

Related commands

display voice-vlan state

voice-vlan track lldp

Use **voice-vlan track lldp** to enable LLDP for automatic IP phone discovery.

Use **undo voice-vlan track lldp** to disable LLDP for automatic IP phone discovery.

Syntax

voice-vlan track lldp

undo voice-vlan track lldp

Views

System view

Default

LLDP for automatic IP phone discovery is disabled.

Predefined user roles

network-admin

Examples

Enable LLDP for automatic IP phone discovery.

```
<Sysname> system-view
[Sysname] voice-vlan track lldp
```

Contents

MVRP commands

display mvrp running-status

Use **display mvrp running-status** to display MVRP running status.

Syntax

display mvrp running-status [**interface** *interface-list*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-list*: Specifies a range of Ethernet interfaces in the form of *interface-type interface-number1* [**to** *interface-type interface-number2*]. The *interface-type interface-number* argument represents the interface type and interface number. The value for the *interface-number2* argument must be greater than or equal to the value for the *interface-number1* argument. If the specified interfaces are not enabled with MVRP, this command displays global MVRP information. If you do not specify this option, the command displays global MVRP information and MVRP running status for all MVRP-enabled ports.

Examples

Display global MVRP information and MVRP running status for all MVRP-enabled ports.

```
<Sysname> display mvrp running-status
 -------[MVRP Global Info]-------
 Global Status     : Enabled
 Compliance-GVRP   : False

 ----[GigabitEthernet1/0/1]----
 Config Status                  : Enabled
 Running Status                 : Enabled
 Join Timer                     : 20 (centiseconds)
 Leave Timer                    : 60 (centiseconds)
 Periodic Timer                 : 100 (centiseconds)
 LeaveAll Timer                 : 1000 (centiseconds)
 Registration Type              : Normal
 Registered VLANs :
  1(default), 2-10
 Declared VLANs :
  1(default), 2-10
 Propagated VLANs :
  1(default), 2-10

 ----[GigabitEthernet1/0/2]----
 Config Status                  : Enabled
```

```
Running Status                  : Disabled
Join Timer                      : 20 (centiseconds)
Leave Timer                     : 60 (centiseconds)
Periodic Timer                  : 100 (centiseconds)
LeaveAll Timer                  : 1000 (centiseconds)
Registration Type               : Normal
Registered VLANs :
 None
Declared  VLANs :
 None
Propagated VLANs :
 None
```

Table 1 Command output

Field	Description
MVRP Global Info	Global MVRP information.
Global Status	Global MVRP status: • Enabled. • Disabled.
Compliance-GVRP	GVRP compatibility status: • **True**—Compatible. • **False**—Incompatible.
Config Status	Whether MVRP is enabled on the port: • Enabled. • Disabled.
Running Status	Whether MVRP takes effect on the port: • **Enabled**—MVRP takes effect on the port. • **Disabled**—MVRP does not take effect on the port. Whether MVRP takes effect on a port is determined by the following items: • Global and port-specific MVRP enabling status. • Physical link state of the port. • Port link type. • Whether the port is a member of an aggregation group.
Registration Type	MVRP registration mode: • Normal. • Fixed. • Forbidden.
Registered VLANs	VLANs that the port has registered.
Declared VLANs	VLANs that the port has declared to its peer participant.
Propagated VLANs	VLANs that the port has learned and notified other participants on the same device to declare to their respective peer participants.

display mvrp state

Use **`display mvrp state`** to display the MVRP state of a port in a VLAN.

Syntax

display mvrp state interface *interface-type interface-number* **vlan** *vlan-id*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

Examples

Display the MVRP state of GigabitEthernet 1/0/1 in VLAN 2.

```
<Sysname> display mvrp state interface gigabitethernet 1/0/1 vlan 2
 MVRP state of VLAN 2 on port GE1/0/1:
 Port                      VLAN   App-state   Reg-state
 ------------------------ ------ ----------- -----------
 GE1/0/1                     2       VP          IN
```

Table 2 Command output

Field	Description
MVRP state of VLAN 2 on port GE1/0/1	MVRP state of GigabitEthernet 1/0/1 in VLAN 2.
App-state	State of the attribute that the local participant declares to its peer participant: • **VO**—Very anxious observer. • **VP**—Very anxious passive. • **VN**—Very anxious new. • **AN**—Anxious new. • **AA**—Anxious active. • **QA**—Quiet active. • **LA**—Leaving active. • **AO**—Anxious observer. • **QO**—Quiet observer. • **AP**—Anxious passive. • **QP**—Quiet passive. • **LO**—Leaving observer.
Reg-state	Registration state of the attribute declared by the peer participant on the local participant: • **IN**—The attribute is registered. • **LV**—The attribute is previously registered, but now it is being deregistered. • **MT**—The attribute is not registered.

display mvrp statistics

Use **display mvrp statistics** to display MVRP statistics.

Syntax

display mvrp statistics [**interface** *interface-list*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-list*: Specifies a range of Ethernet interfaces in the form of *interface-type interface-number1* [**to** *interface-type interface-number2*]. The *interface-type interface-number* argument represents the interface type and interface number. The value for the *interface-number2* argument must be greater than or equal to the value for the *interface-number1* argument. If you do not specify this option, the command displays MVRP statistics of all MVRP-enabled ports.

Usage guidelines

If MVRP is disabled on the specified ports, this command does not provide any output.

Examples

Display MVRP statistics of all ports.

```
<Sysname> display mvrp statistics

 ----[GigabitEthernet1/0/1]----
 Failed Registrations        : 1
 Last PDU Origin             : 000f-e200-0010
 Frames Received             : 201
  New Event Received          : 0
  JoinIn Event Received       : 1167
  In Event Received           : 0
  JoinMt Event Received       : 22387
  Mt Event Received           : 31
  Leave Event Received        : 210
  LeaveAll Event Received     : 63
 Frames Transmitted          : 120
  New Event Transmitted       : 0
  JoinIn Event Transmitted    : 311
  In Event Transmitted        : 0
  JoinMt Event Transmitted    : 873
  Mt Event Transmitted        : 11065
  Leave Event Transmitted     : 167
  LeaveAll Event Transmitted  : 4
 Frames Discarded            : 0

 ----[GigabitEthernet1/0/2]----
 Failed Registrations        : 0
 Last PDU Origin             : 0000-0000-0000
 Frames Received             : 0
  New Event Received          : 0
```

```
  JoinIn Event Received       : 0
  In Event Received           : 0
  JoinMt Event Received       : 0
  Mt Event Received           : 0
  Leave Event Received        : 0
  LeaveAll Event Received     : 0
 Frames Transmitted          : 0
  New Event Transmitted       : 0
  JoinIn Event Transmitted    : 0
  In Event Transmitted        : 0
  JoinMt Event Transmitted    : 0
  Mt Event Transmitted        : 0
  Leave Event Transmitted     : 0
  LeaveAll Event Transmitted  : 0
 Frames Discarded            : 0
```

Table 3 Command output

Field	Description
Failed Registrations	Number of VLAN registration failures through MVRP on the local participant.
Last PDU Origin	Source MAC address of the last MVRPDU.
Frames Received	Number of MVRP frames received.
New Event Received	Number of New events received.
JoinIn Event Received	Number of JoinIn events received.
In Event Received	Number of In events received.
JoinMt Event Received	Number of JoinMt events received.
Mt Event Received	Number of Mt events received.
Leave Event Received	Number of Leave events received.
LeaveAll Event Received	Number of LeaveAll events received.
Frames Transmitted	Number of MVRP frames sent.
New Event Transmitted	Number of New events sent.
JoinIn Event Transmitted	Number of JoinIn events sent.
In Event Transmitted	Number of In events sent.
JoinMt Event Transmitted	Number of JoinMt events sent.
Mt Event Transmitted	Number of Mt events sent.
Leave Event Transmitted	Number of Leave events sent.
LeaveAll Event Transmitted	Number of LeaveAll events sent.
Frames Discarded	Number of MVRP frames dropped.

mrp timer join

Use **mrp timer join** to set the Join timer.

Use **undo mrp timer join** to restore the default.

Syntax

mrp timer join *timer-value*

undo mrp timer join

Default

The Join timer is 20 centiseconds.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

timer-value: Specifies the Join timer value (in centiseconds). The Join timer must meet the following requirements:

- Not less than 20 centiseconds.
- Less than half the Leave timer.
- Divisible by 20 centiseconds.

Examples

Set the Join timer to 40 centiseconds. (In this example, the Leave timer is 100 centiseconds.)

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mrp timer join 40
```

Related commands

display mvrp running-status

mrp timer leave

mrp timer leave

Use **mrp timer leave** to set the Leave timer.

Use **undo mrp timer leave** to restore the default.

Syntax

mrp timer leave *timer-value*

undo mrp timer leave

Default

The Leave timer is 60 centiseconds.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

timer-value: Specifies the Leave timer value (in centiseconds). The Leave timer must meet the following requirements:

- Greater than two times the Join timer.
- Less than the LeaveAll timer.
- Divisible by 20 centiseconds.

Examples

Set the Leave timer to 100 centiseconds. (In this example, the Join timer and LeaveAll timer use their default settings.)

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mrp timer leave 100
```

Related commands

display mvrp running-status

mrp timer join

mrp timer leaveall

mrp timer leaveall

Use **mrp timer leaveall** to set the LeaveAll timer.

Use **undo mrp timer leaveall** to restore the default.

Syntax

mrp timer leaveall *timer-value*

undo mrp timer leaveall

Default

The LeaveAll timer is 1000 centiseconds.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameter

timer-value: Specifies the LeaveAll timer value (in centiseconds). The LeaveAll timer must meet the following requirements:

- Greater than any Leave timer on each port.
- Not greater than 32760 centiseconds.
- Divisible by 20 centiseconds.

Usage guidelines

Each time the LeaveAll timer of a port expires, all attributes of the MSTIs on the port are deregistered throughout the network. To prevent this type of deregistration from affecting the network, do not set the LeaveAll timer to less than its default value.

To keep the dynamic VLANs learned through MVRP stable, do not set the LeaveAll timer less than its default value.

The device randomly changes the LeaveAll timer within a certain range when an MRP participant restarts its LeaveAll timer. This prevents the LeaveAll timer of a particular participant from always expiring first.

Examples

Set the LeaveAll timer to 1500 centiseconds. (In this example, the Leave timer on each port uses the default setting.)

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mrp timer leaveall 1500
```

Related commands

display mvrp running-status

mrp timer leave

mrp timer periodic

Use **mrp timer periodic** to set the Periodic timer.

Use **undo mrp timer periodic** to restore the default.

Syntax

mrp timer periodic *timer-value*

undo mrp timer periodic

Default

The Periodic timer is 100 centiseconds.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

timer-value: Specifies the Periodic timer, which can be 0 or 100 centiseconds.

Usage guidelines

Setting the Periodic timer to 0 disables the Periodic timer.

Setting the Periodic timer to 100 enables the Periodic timer. The participant then sends MRP frames at an interval of 100 centiseconds.

Examples

Disable the Periodic timer.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mrp timer periodic 0
```

Related commands

display mvrp running-status

mvrp enable

Use **mvrp enable** to enable MVRP on a port.

Use **undo mvrp enable** to disable MVRP on a port.

Syntax

mvrp enable

undo mvrp enable

Default

MVRP is disabled on a port.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

For MVRP to take effect on a port, make sure the following requirements are met:

- MVRP is enabled both globally and on the port.
- The port is physically up.
- The port link type is trunk.
- The port is not a member of an aggregation group.

Examples

Enable MVRP on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] mvrp global enable
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
[Sysname-GigabitEthernet1/0/1] mvrp enable
```

Related commands

display mvrp running-status

mvrp global enable

Use **mvrp global enable** to enable MVRP globally.

Use **undo mvrp global enable** to disable MVRP globally.

Syntax

mvrp global enable

undo mvrp global enable

Default

MVRP is disabled globally.

Views

System view

Predefined user roles

network-admin

Usage guidelines

For MVRP to take effect on a port, enable MVRP both on the port and globally.

Examples

Enable MVRP globally.

```
<Sysname> system-view
[Sysname] mvrp global enable
```

Related commands

display mvrp running-status

mvrp gvrp-compliance enable

Use **mvrp gvrp-compliance enable** to enable GVRP compatibility for MVRP.

Use **undo mvrp gvrp-compliance enable** to restore the default.

Syntax

mvrp gvrp-compliance enable

undo mvrp gvrp-compliance enable

Default

MVRP is incompatible with GVRP.

Views

System view

Predefined user roles

network-admin

Usage guidelines

When you enable GVRP compatibility for MVRP, the device can receive and send both MVRP and GVRP frames.

Examples

Enable GVRP compatibility for MVRP.

```
<Sysname> system-view
[Sysname] mvrp gvrp-compliance enable
```

Related commands

display mvrp running-status

mvrp registration

Use **mvrp registration** to set the MVRP registration mode on a port.

Use **undo mvrp registration** to restore the default.

Syntax

mvrp registration { **fixed** | **forbidden** | **normal** }

undo mvrp registration

Default

The MVRP registration mode is normal.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

fixed: Specifies the fixed registration mode.

forbidden: Specifies the forbidden registration mode.

normal: Specifies the normal registration mode.

Examples

Set the MVRP registration mode to fixed on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mvrp registration fixed
```

Related commands

display mvrp running-status

reset mvrp statistics

Use **reset mvrp statistics** to clear MVRP statistics for ports.

Syntax

reset mvrp statistics [**interface** *interface-list*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-list*: Specifies a range of Ethernet interfaces in the form of *interface-type interface-number1* [**to** *interface-type interface-number2*]. The *interface-type interface-number* argument represents the interface type and interface number. The value for the *interface-number2* argument must be greater than or equal to the value for the *interface-number1* argument. If you do not specify this option, the command clears MVRP statistics of all ports.

Examples

Clear MVRP statistics for all ports.

```
<Sysname> reset mvrp statistics
```

Related commands

display mvrp statistics

Contents

QinQ commands

The S5110V2-SI, S5000V3-EI, S5000V5-EI, S5000E-X, S5000X-EI, and WAS6000 switch series do not support QinQ.

This document uses the following terms:

- **CVLAN**—Customer network VLANs, also called inner VLANs, refer to VLANs that a customer uses on the private network.
- **SVLAN**—Service provider network VLANs, also called outer VLANs, refer to VLANs that a service provider uses to transmit VLAN tagged traffic for customers.

display qinq

Use **display qinq** to display QinQ-enabled interfaces.

Syntax

display qinq [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays all QinQ-enabled interfaces.

Usage guidelines

If QinQ is not enabled on any interfaces, this command does not provide any output.

Examples

Enable QinQ on GigabitEthernet 1/0/1. Then, verify that QinQ is enabled on the interface.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qinq enable
[Sysname-GigabitEthernet1/0/1] display qinq interface gigabitethernet 1/0/1
Interface
 GigabitEthernet1/0/1
```

Enable QinQ on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/3. Then, verify that QinQ is enabled on the interfaces.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qinq enable
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] interface gigabitethernet 1/0/3
[Sysname-GigabitEthernet1/0/3] qinq enable
[Sysname-GigabitEthernet1/0/3] display qinq
Interface
```

```
GigabitEthernet1/0/1
GigabitEthernet1/0/3
```

Related commands

qinq enable

qinq enable

Use **qinq enable** to enable QinQ on an interface.

Use **undo qinq enable** to disable QinQ on an interface.

Syntax

qinq enable

undo qinq enable

Default

QinQ is disabled on interfaces.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Examples

Enable QinQ on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qinq enable
```

Related commands

display qinq

qinq ethernet-type (interface view)

Use **qinq ethernet-type** to set the TPID value in SVLAN tags on an interface.

Use **undo qinq ethernet-type** to restore the default TPID value in SVLAN tags on an interface.

Syntax

qinq ethernet-type service-tag *hex-value*

undo qinq ethernet-type service-tag

Default

The TPID value in SVLAN tags is 8100 in hexadecimal notation.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

service-tag: Sets the TPID value in the SVLAN tag.

hex-value: Sets a hexadecimal TPID value in the range of 1 to ffff, excluding the reserved EtherType values listed in Table 1.

Table 1 Reserved EtherType values

Protocol type	Value
ARP	0x0806
PUP	0x0200
RARP	0x8035
IP	0x0800
IPv6	0x86dd
PPPoE	0x8863/0x8864
MPLS	0x8847/0x8848
IPX/SPX	0x8137
IS-IS	0x8000
LACP	0x8809
LLDP	0x88cc
802.1X	0x888e
802.1ag	0x8902
Cluster	0x88a7
Reserved	0xfffd/0xfffe/0xffff

Usage guidelines

A port without QinQ enabled uses the SVLAN TPID to match incoming tagged frames. The port modifies the TPID in the SVLAN tag of outgoing frames as the configured value.

Examples

Set the TPID value in SVLAN tags to 9100 (hexadecimal) on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qinq ethernet-type service-tag 9100
```

Related commands

qinq ethernet-type (system view)

qinq ethernet-type (system view)

Use **qinq ethernet-type** to set the TPID value in CVLAN tags.

Use **undo qinq ethernet-type** to restore the default TPID value in CVLAN tags.

Syntax

qinq ethernet-type customer-tag *hex-value*

undo qinq ethernet-type customer-tag

Default

The TPID value in CVLAN tags is 8100 in hexadecimal notation.

Views

System view

Predefined user roles

network-admin

Parameters

customer-tag: Sets the TPID value in the CVLAN tag.

hex-value: Sets a hexadecimal TPID value in the range of 1 to ffff, excluding the reserved EtherType values listed in Table 2.

Table 2 Reserved EtherType values

Protocol type	Value
ARP	0x0806
PUP	0x0200
RARP	0x8035
IP	0x0800
IPv6	0x86dd
PPPoE	0x8863/0x8864
MPLS	0x8847/0x8848
IPX/SPX	0x8137
IS-IS	0x8000
LACP	0x8809
LLDP	0x88cc
802.1X	0x888e
802.1ag	0x8902
Cluster	0x88a7
Reserved	0xfffd/0xfffe/0xffff

Examples

Set the TPID value in CVLAN tags to 8200 (hexadecimal).

```
<Sysname> system-view
[Sysname] qinq ethernet-type customer-tag 8200
```

Related commands

qinq ethernet-type (interface view)

qinq transparent-vlan

Use **qinq transparent-vlan** to enable transparent transmission for a list of VLANs on a port.

Use **undo qinq transparent-vlan** to disable transparent transmission for a list of VLANs on a port.

Syntax

qinq transparent-vlan *vlan-id-list*

undo qinq transparent-vlan { *vlan-id-list* | **all** }

Default

Transparent transmission is disabled for all VLANs.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a single VLAN ID or a VLAN ID range in the form of *vlan-id1* **to** *vlan-id2*. The value range for VLAN IDs is 1 to 4094. The end VLAN ID must be equal to or greater than the start VLAN ID.

all: Specifies all VLANs.

Usage guidelines

By default, QinQ tags all incoming frames with the PVID on a port. This command disables QinQ to tag incoming traffic from a list of VLANs. These VLANs are called transparent VLANs.

You can repeat this command to add VLANs to the list of transparent VLANs.

To ensure successful transmission for a transparent VLAN, follow these configuration guidelines:

- Set the link type of the port to trunk or hybrid, and assign the port to the transparent VLAN.
- Do not configure any other VLAN manipulation actions for the transparent VLAN on the port.
- Make sure all ports on the traffic path permit the transparent VLAN to pass through.
- If you use both transparent VLANs and VLAN mappings on an interface, the transparent VLANs cannot be the original or translated VLANs of one-to-one or one-to-two VLAN mappings.

Examples

Configure GigabitEthernet 1/0/1 as a trunk port, and assign the port to VLAN 2, VLAN 3, and VLANs 50 through 100. Enable QinQ on GigabitEthernet 1/0/1, and configure the port to transparently transmit frames from VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
[Sysname-GigabitEthernet1/0/1] port trunk permit vlan 2 3 50 to 100
[Sysname-GigabitEthernet1/0/1] qinq enable
[Sysname-GigabitEthernet1/0/1] qinq transparent-vlan 2
```

Contents

VLAN mapping commands

display vlan mapping

Use **display vlan mapping** to display VLAN mapping information.

Syntax

display vlan mapping [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, the command displays VLAN mapping information on all interfaces.

Examples

Display VLAN mapping information on all interfaces.

```
<Sysname> display vlan mapping

Interface GigabitEthernet1/0/1:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  10            N/A           120                      N/A

Interface GigabitEthernet1/0/2:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  1024-4094     N/A           100                      N/A

Interface GigabitEthernet1/0/3:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  12            N/A           110                      12
```

Table 1 Command output

Field	Description
Outer VLAN	Original outer VLAN. This field indicates the original VLAN for a one-to-one, many-to-one, or one-to-two VLAN mapping.
Inner VLAN	Original inner VLAN. This field displays **N/A** for a one-to-one, many-to-one, or one-to-two VLAN mapping.
Translated Outer VLAN	Translated outer VLAN. This field indicates the translated VLAN for a one-to-one or

Field	Description
	many-to-one VLAN mapping. This field indicates the SVLAN to be added for a one-to-two VLAN mapping.
Translated Inner VLAN	Translated inner VLAN. This field displays **N/A** for a one-to-one or many-to-one VLAN mapping.

Related commands

vlan mapping

vlan mapping

Use **vlan mapping** to configure VLAN mapping on an interface.

Use **undo vlan mapping** to cancel the VLAN mapping configuration.

NOTE:

Many-to-one VLAN mapping is supported only in Release 6350 and later.

Syntax

vlan mapping { *vlan-id* **translated-vlan** *vlan-id* | **nest** { **range** *vlan-range-list* | **single** *vlan-id-list* } **nested-vlan** *vlan-id* | **uni** { **range** *vlan-range-list* | **single** *vlan-id-list* } **translated-vlan** *vlan-id* }

undo vlan mapping { *vlan-id* **translated-vlan** *vlan-id* | **all** | **nest** { **range** *vlan-range-list* | **single** *vlan-id-list* } **nested-vlan** *vlan-id* | **uni** { **range** *vlan-range-list* | **single** *vlan-id-list* } **translated-vlan** *vlan-id* }

Default

No VLAN mapping is configured on an interface.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan-id **translated-vlan** *vlan-id*: Specifies the original VLAN and translated VLAN for a one-to-one VLAN mapping. The value range for the *vlan-id* argument is 1 to 4094. The original VLAN and the translated VLAN cannot be the same.

uni range *vlan-range-list* **translated-vlan** *vlan-id*: Specifies the original VLAN ranges and the translated VLAN for a many-to-one VLAN mapping on the customer-side port. The *vlan-range-list* argument specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN ID or a range of VLAN IDs in the form of *vlan-id1* **to** *vlan-id2*. The value range for VLAN IDs is 1 to 4094. The value for the *vlan-id2* argument must be greater than the value for the *vlan-id1* argument. The value range for the *vlan-id* argument is 1 to 4094. Different VLAN ranges cannot overlap. Any of the original VLANs cannot be the same as the translated VLAN.

uni single *vlan-id-list* **translated-vlan** *vlan-id*: Specifies the original VLANs and the translated VLAN for a many-to-one VLAN mapping on the customer-side port. The

vlan-id-list argument specifies a space-separated list of up to 10 VLAN IDs, each of which is in the range of 1 to 4094. The value range for the *vlan-id* argument is 1 to 4094. Any of the original VLANs cannot be the same as the translated VLAN.

nest range *vlan-range-list* **nested-vlan** *vlan-id*: Specifies the CVLAN ranges and the SVLAN for a one-to-two VLAN mapping. The *vlan-range-list* argument specifies a space-separated list of up to 10 CVLAN items. Each item specifies a CVLAN ID or a range of CVLAN IDs in the format of *vlan-id1* **to** *vlan-id2*. The value range for CVLAN IDs is 1 to 4094. The value for the *vlan-id2* argument must be greater than the value for the *vlan-id1* argument. Different CVLAN ranges cannot overlap. The *vlan-id* argument specifies the SVLAN ID in the range of 1 to 4094.

nest single *vlan-id-list* **nested-vlan** *vlan-id*: Specifies the CVLANs and the SVLAN for a one-to-two VLAN mapping. The *vlan-id-list* argument specifies a space-separated list of up to 10 CVLAN IDs, each of which is in the range of 1 to 4094. The *vlan-id* argument specifies the SVLAN ID in the range of 1 to 4094.

all: Deletes all VLAN mapping configurations from the interface.

Usage guidelines

VLAN mapping takes effect only on VLAN-tagged packets received on an interface.

The original and translated VLANs in VLAN mappings on the same interface must meet the following requirements:

- Different types of VLAN mapping entries cannot include the same original VLANs or translated VLANs.
- Different one-to-one VLAN mapping entries cannot include the same translated VLANs. If you configure multiple one-to-one VLAN mapping entries for the same original VLANs, the most recent configuration takes effect.

Before you enable or disable QinQ on a port, you must remove all VLAN mappings on the port.

If you use both transparent VLANs and VLAN mappings on an interface, the transparent VLANs cannot be the following VLANs:

- Original or translated VLANs of one-to-one and one-to-two VLAN mappings.

The MTU of an interface is 1500 bytes by default. After a VLAN tag is added to a packet, the packet length is added by 4 bytes. As a best practice, set the MTU to a minimum of 1504 bytes for ports on the forwarding path of the packet on the service provider network.

Examples

Configure a one-to-one VLAN mapping on GigabitEthernet 1/0/1 to map VLAN 1 to VLAN 101.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] vlan mapping 1 translated-vlan 101
```

Configure many-to-one VLAN mappings on the customer-side port (GigabitEthernet 1/0/2) to map VLANs 1 through 50 and 80 to VLAN 101.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] vlan mapping uni range 1 to 50 translated-vlan 101
[Sysname-GigabitEthernet1/0/2] vlan mapping uni single 80 translated-vlan 101
```

Configure one-to-two VLAN mappings on GigabitEthernet 1/0/4 to add SVLAN tag 101 to packets carrying VLAN tags 1 through 10 and VLAN tag 80.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/4
[Sysname-GigabitEthernet1/0/4] vlan mapping nest range 1 to 10 nested-vlan 101
```

```
[Sysname-GigabitEthernet1/0/4] vlan mapping nest single 80 nested-vlan 101
```

Related commands

display vlan mapping

Contents

LLDP commands

cdp voice-vlan

Use **cdp voice-vlan** to set the voice VLAN ID carried in CDP frames.

Use **undo cdp voice-vlan** to restore the default.

NOTE:

This command is not available on the S5110V2-SI, S5000V3-EI, S5000V5-EI, S5000E-X, S5000X-EI, or WAS6000 switch series.

Syntax

cdp voice-vlan *vlan-id*

undo cdp voice-vlan

Default

No voice VLAN ID is configured to be carried in CDP frames.

Views

Layer 2 Ethernet interface view

Default command level

network-admin

Parameters

vlan-id: Specifies a voice VLAN ID to be advertised, in the range of 1 to 4094.

Usage guidelines

With this command configured, CDP frames sent to IP phones from the interface carry the voice VLAN ID specified in this command. IP phones use the voice VLAN ID to send voice traffic.

Examples

Set the voice VLAN ID carried in CDP frames to 100.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] cdp voice-vlan 100
```

display lldp local-information

Use **display lldp local-information** to display local LLDP information.

Syntax

display lldp local-information [**global** | **interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

global: Displays the global local LLDP information.

interface *interface-type interface-number*: Specifies a port by its type and number.

Usage guidelines

If you do not specify any keywords or arguments, the command displays all local LLDP information, which includes the following:

- The global LLDP information.
- The LLDP information about the LLDP-enabled ports in up state.

Examples

Display all local LLDP information.

```
<Sysname> display lldp local-information
Global LLDP local-information:
 Chassis ID          : 00e0-fc00-5600
 System name         : Sysname
H3C Comware Platform Software, Software Version 7.1.070, Release 6340
   H3C S5130S-52S-HI
   Copyright (c) 2004-2022 New H3C Technologies Co., Ltd. All rights reserved.
 System capabilities supported  : Bridge, Router, Customer Bridge, Service Bridge
 System capabilities enabled    : Bridge, Router, Service Bridge
 MED information:
 Device class               : Connectivity device
 MED inventory information of master board:
 HardwareRev                : REV.A
 FirmwareRev                : 109
 SoftwareRev                : 7.1.070 Release 6340
 SerialNum                  : NONE
 Manufacturer name          : H3C
 Model name                 : H3C S5130S-52S-HI
 Asset tracking identifier  : Unknown
LLDP local-information of port 3[GigabitEthernet1/0/3]:
 Port ID type       : Interface name
 Port ID            : GigabitEthernet1/0/3
 Port description   : GigabitEthernet1/0/3 Interface
 LLDP agent nearest-bridge management address:
 Management address type           : IPv4
 Management address                : 192.168.80.60
 Management address interface type : IfIndex
 Management address interface ID   : Unknown
 Management address OID            : 0
 LLDP agent nearest-nontpmr management address:
 Management address type           : IPv4
 Management address                : 192.168.80.61
 Management address interface type : IfIndex
 Management address interface ID   : Unknown
 Management address OID            : 0
```

```
LLDP agent nearest-customer management address:
Management address type           : IPv4
Management address                : 192.168.80.62
Management address interface type : IfIndex
Management address interface ID   : Unknown
Management address OID            : 0
Port VLAN ID(PVID): 1
Port and protocol VLAN ID(PPVID) : 12
Port and protocol VLAN supported : Yes
Port and protocol VLAN enabled   : Yes
VLAN name of VLAN 12: VLAN 0012
Management VLAN ID  : 5
Link aggregation supported : Yes
Link aggregation enabled   : No
Aggregation port ID        : 0
Auto-negotiation supported : Yes
Auto-negotiation enabled   : Yes
OperMau                    : Speed(1000)/Duplex(Full)
Power port class           : PSE
PSE power supported        : NO
PSE power enabled          : NO
PSE pairs control ability  : NO
Power pairs                : Signal
Port power classification  : Class 0
Maximum frame size         : 10000
Transmit Tw                : 0 us
Receive Tw                 : 0 us
Fallback Tw                : 0 us
Echo Transmit Tw           : 0 us
Echo Receive Tw            : 0 us
PoE PSE power source       : Primary
Port PSE priority          : Critical
Port available power value : 0.0 w
PoE power information:
 Current power             : 11592 mW
 Average power             : 11610 mW
 Peak power                : 11684 mW
 Max Power                 : 100000 mW
 Current                   : 0 mA
```

Table 1 Command output

Field	Description
Chassis ID	Bridge MAC address of the device.
System capabilities supported	Supported capabilities: • **Bridge**—Switching is supported. • **Router**—Routing is supported. • **Repeater**—Signal repeating is supported. • **Telephone**—The local device can act as a telephone.

Field	Description
	• **DocsisCableDevice**—The local device can act as a DOCSIS-compliant cable device. • **StationOnly**—The local device can act as a station only. • **Customer Bridge**—The customer bridge feature is supported. • **Service Bridge**—The service bridge feature is supported. • **TPMR**—The TPMR feature is supported. • **Other**—Features other than those listed above are supported.
System capabilities enabled	Enabled capabilities: • **Bridge**—Switching is enabled. • **Router**—Routing is enabled. • **Repeater**—Signal repeating is enabled. • **Telephone**—The local device is acting as a telephone. • **DocsisCableDevice**—The local device is acting as a DOCSIS-compliant cable device. • **StationOnly**—The local device is acting as a station only. • **Customer Bridge**—The customer bridge feature is enabled. • **Service Bridge**—The service bridge feature is enabled. • **TPMR**—The TPMR feature is enabled. • **Other**—Features other than those listed above are enabled.
Device class	MED device class: • **Connectivity device**—Network device. • **Class I**—Normal terminal device. It requires the basic LLDP discovery services. • **Class II**—Media terminal device. It supports media streams, and can also act as a normal terminal device. • **Class III**—Communication terminal device. It supports the IP communication systems of end users, and can also act as a normal terminal device or media terminal device.
MED inventory information of master board	MED inventory information about the .
HardwareRev	Hardware version.
FirmwareRev	Firmware version.
SoftwareRev	Software version.
SerialNum	Serial number.
Manufacturer name	Device manufacturer.
Model name	Device model.
Port ID type	Port ID type: • MAC address. • Interface name.
Port ID	Port ID, the value of which depends on the port ID type.
Management address interface type	Numbering type of the interface identified by the management address.
Management address interface ID	Index of the interface identified by the management address.
Management address OID	Management address object ID.
Port VLAN ID(PVID)	Port PVID.

Field	Description
Port and protocol VLAN ID(PPVID)	Port protocol VLAN ID.
Port and protocol VLAN supported	Indicates whether protocol VLAN is supported on the port.
Port and protocol VLAN enabled	Indicates whether protocol VLAN is enabled on the port.
Link aggregation supported	Indicates whether link aggregation is supported on the port.
Link aggregation enabled	Indicates whether link aggregation is enabled on the port.
Aggregation port ID	Member port ID, which is 0 when link aggregation is disabled.
Auto-negotiation supported	Indicates whether autonegotiation is supported on the port.
Auto-negotiation enabled	Indicates whether autonegotiation is enabled on the port.
OperMau	Speed and duplex state of the port.
Power port class	PoE port class: • **PSE**—Power sourcing equipment. • **PD**—Powered device.
PSE power supported	Indicates whether the device can operate as a PSE.
PSE power enabled	Indicates whether the device is operating as a PSE.
PSE pairs control ability	Indicates whether the pair selection ability is available.
Power pairs	Power supply mode: • **Signal**—Uses data pairs to supply power. • **Spare**—Uses spare pairs to supply power.
Port power classification	Power class of the PD: • Class 0. • Class 1. • Class 2. • Class 3. • Class 4.
PoE PSE power source	PSE power source type: • **Unknown**—Unknown power supply. • **Primary**—Primary power supply. • **Backup**—Backup power supply.
PoE PD power source	PD power source type: • **Unknown**—Unknown power supply. • **PSE**—PSE power supply. • **Local**—Local power supply. • **PSE and local**—PSE and local power supplies.
Port PSE priority	PoE power supply priority of PSE ports: • Unknown. • Critical. • High. • Low.
Port PD priority	PoE power receiving priority of PD ports: • Unknown. • Critical. • High.

Field	Description
	• Low.
Port available power value	Available PoE power on PSE ports, or power needed on PD ports, in watts.
Transmit Tw	Sleep time of the local client, in μs.
Receive Tw	Sleep time of the peer client expected by the local client, in μs.
Fallback Tw	Candidate sleep time of the peer client expected by the local client, in μs.
Echo Transmit Tw	Sleep time of the peer client, in μs. This field displays zero when one of the following cases occurs: • The local client has not received the sleep time of the peer client. • The sleep time of the peer client is 0 μs.
Echo Receive Tw	Sleep time of the local client expected by the peer client, in μs. This field displays zero when one of the following cases occurs: • The local client has not received the expected sleep time from the peer client. • The sleep time of the local client expected by the peer client is 0 μs.
Current power	Current power of a PoE interface, including PD consumption power and transmission loss.
Average power	Average power of a PoE interface.
Peak power	Peak power of a PoE interface.
Max Power	This field is supported only in R6350 and later. Maximum power of a PoE interface.
Current	This field is supported only in R6350 and later. Current of a PoE interface at the moment, in mA.

display lldp neighbor-information

Use **display lldp neighbor-information** to display the LLDP information received from the neighboring devices.

Syntax

display lldp neighbor-information [[[**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** | **nearest-nontpmr** }] [**verbose**]] | **list** [**system-name** *system-name*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify this option, the command displays the LLDP information that all ports receive from the neighboring devices.

agent: Specifies an agent type. If you do not specify an agent type, the command displays the LLDP information that all LLDP agents receive from the neighboring devices.

nearest-bridge: Specifies nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

verbose: Displays the detailed LLDP information that the local device receives from the neighboring devices. If you do not specify this keyword, the command displays the brief LLDP information that the local device receives from the neighboring devices.

list: Displays the LLDP information that the local device receives from the neighboring devices in the form of a list.

system-name *system-name*: Displays the LLDP information that the local device receives from a neighboring device specified by its system name. The *system-name* argument is a string of 1 to 255 characters. If you do not specify this option, the command displays the LLDP information that the local device receives from all neighboring devices in a list.

Examples

Display detailed LLDP information that the nearest bridge agents on all ports received from the neighboring devices.

```
<Sysname> display lldp neighbor-information agent nearest-bridge verbose
LLDP neighbor-information of port 1[GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
 LLDP Neighbor index : 1
 Update time         : 0 days, 0 hours, 1 minutes, 1 seconds
 Chassis type        : MAC address
 Chassis ID          : 000f-0055-0002
 Port ID type        : Interface name
 Port ID             : GigabitEthernet1/0/1
 Time to live        : 121
 Port description    : GigabitEthernet1/0/1 Interface
 System name         : Sysname
   H3C Comware Platform Software, Software Version 7.1.070, Release 6342
   H3C S5130S-52S-HI
   Copyright (c) 2004-2022 New H3C Technologies Co., Ltd. All rights reserved.
 System capabilities supported : Bridge, Router, Customer Bridge, Service Bridge
 System capabilities enabled   : Bridge, Router, Customer Bridge
 Management address type           : IPv4
 Management address                : 192.168.1.55
 Management address interface type : IfIndex
 Management address interface ID   : Unknown
 Management address OID            : 0
 Port VLAN ID(PVID): 1
 Link aggregation supported : Yes
 Link aggregation enabled   : No
 Aggregation port ID        : 0
 Management VLAN ID  : 5
 Auto-negotiation supported : Yes
 Auto-negotiation enabled   : Yes
 OperMau                    : Speed(1000)/Duplex(Full)
 Power port class           : PD
 PSE power supported        : Yes
```

```
 PSE power enabled          : Yes
 PSE pairs control ability  : Yes
 Power pairs                : Signal
 Port power classification  : Class 0
 Maximum frame size         : 9216
```

Display brief LLDP information that all LLDP agents received from all neighboring devices.

```
<Sysname> display lldp neighbor-information
LLDP neighbor-information of port 3[GigabitEthernet1/0/3]:
LLDP agent nearest-bridge:
 LLDP neighbor index : 3
 ChassisID/subtype   : 0011-2233-4400/MAC address
 PortID/subtype      : 000c-29f5-c71f/MAC address
 Capabilities        : Bridge, Router, Customer Bridge
 LLDP neighbor index : 6
 ChassisID/subtype   : 0011-2233-4400/MAC address
 PortID/subtype      : 000c-29f5-c715/MAC address
 Capabilities        : None
CDP neighbor-information of port 3[GigabitEthernet1/0/3]:
LLDP agent nearest-bridge:
 CDP neighbor index  : 4
 Chassis ID          : SEP00260B5C0548
 Port ID             : Port 1
 CDP neighbor index  : 5
 Chassis ID          : 0011-2233-4400
 Port ID             : GigabitEthernet1/0/4
LLDP neighbor-information of port 3[GigabitEthernet1/0/3]:
LLDP agent nearest-nontpmr:
 LLDP neighbor index : 6
 ChassisID/subtype   : 0011-2233-4400/MAC address
 PortID/subtype      : 000c-29f5-c715/MAC address
 Capabilities        : None
```

Display brief LLDP information that all LLDP agents received from the neighboring devices in a list.

```
<Sysname> display lldp neighbor-information list
Chassis ID : * -- --Nearest nontpmr bridge neighbor
             # -- --Nearest customer bridge neighbor
             Default -- -- Nearest bridge neighbor
Local Interface Chassis ID      Port ID                   System Name
GE1/0/1         000f-e25d-ee91  GigabitEthernet1/0/1      System1
```

Table 2 Command output

Field	Description
LLDP neighbor-information of port 1	LLDP information received through port 1.
Update time	Time when LLDP information about a neighboring device was last updated.
LLDP mac type	Type of the neighbor MAC address: • Nearest bridge. • Nearest customer bridge.

Field	Description
	• Nearest non-TPMR bridge.
Chassis type	Chassis ID type: • **Chassis component**. • **Interface alias**. • **Port component**. • **MAC address**. • **Network address (ipv4)**. • **Interface name**. • **Locally assigned**—Locally-defined chassis type other than those listed above.
Chassis ID	ID that identifies the LLDP sending device, which can be a MAC address, a network address, an interface, or some other value, depending on the chassis ID type of the neighboring device.
Port ID type	Port ID type: • **Interface alias**. • **Port component**. • **MAC address**. • **Network address (ipv4)**. • **Interface name**. • **Agent circuit ID**. • **Locally assigned**—Locally-defined port ID type other than those listed above.
Port ID	Value of the type of the port ID.
System name	System name of the neighboring device.
System description	System description of the neighboring device.
System capabilities supported	Capabilities supported on the neighboring device: • **Repeater**—Signal repeating is supported. • **Bridge**—Switching is supported. • **Router**—Routing is supported. • **Telephone**—The neighboring device can act as a telephone. • **DocsisCableDevice**—The neighboring device can act as a DOCSIS-compliant cable device. • **StationOnly**—The neighboring device can act as a station only. • **Customer Bridge**—The customer bridge feature is enabled. • **Service Bridge**—The service bridge feature is enabled. • **TPMR**—The TPMR feature is enabled. • **Other**—Features other than those listed above are supported.
System capabilities enabled	Capabilities enabled on the neighboring device: • **Repeater**—Signal repeating is enabled. • **Bridge**—Switching is enabled. • **Router**—Routing is enabled. • **Telephone**—The neighboring device is acting as a telephone. • **DocsisCableDevice**—The neighboring device is acting as a DOCSIS-compliant cable device. • **StationOnly**—The neighboring device is acting as a station only. • **Customer Bridge**—The customer bridge feature is enabled. • **Service Bridge**—The service bridge feature is enabled.

Field	Description
	• **TPMR**—The TPMR feature is enabled. • **Other**—Features other than those listed above are supported.
Management address OID	Management address object ID.
Link aggregation supported	Indicates whether link aggregation is supported.
Link aggregation enabled	Indicates whether link aggregation is enabled.
Aggregation port ID	Member port ID, which is 0 when link aggregation is disabled.
Auto-negotiation supported	Indicates whether autonegotiation is supported on the port.
Auto-negotiation enabled	Indicates whether autonegotiation is enabled on the port.
OperMau	Speed and duplex state on the port.
Power port class	PoE port class: • **PSE**—Power sourcing equipment. • **PD**—Powered device.
PSE power supported	Indicates whether the device can operate as a PSE.
PSE power enabled	Indicates whether the device is operating as a PSE.
PSE pairs control ability	Indicates whether the pair selection ability is available.
Power pairs	Power supply mode: • **Signal**—Uses data pairs to supply power. • **Spare**—Uses spare pairs to supply power.
Port power classification	Power class of the PD: • Class 0. • Class 1. • Class 2. • Class 3. • Class 4.
TLV type	Unknown basic TLV type.
TLV information	Information contained in the unknown basic TLV type.
Unknown organizationally-defined TLV	Unknown organizationally specific TLV.
TLV OUI	OUI of the unknown organizationally specific TLV.
TLV subtype	Unknown organizationally specific TLV subtype.
Index	Unknown organization index.
Capabilities	Capabilities enabled on the neighboring device: • **Repeater**—Signal repeating is enabled. • **Bridge**—Switching is enabled. • **Router**—Routing is enabled. • **Telephone**—The neighboring device is acting as a telephone. • **DocsisCableDevice**—The neighboring device is acting as a DOCSIS-compliant cable device. • **StationOnly**—The neighboring device is acting as a station only. • **Other**—Features other than those listed above are supported. • **None**—The neighboring device does not advertise this TLV.
Local Interface	Local port that receives the LLDP information.

Field	Description
Chassis ID : * -- -- Nearest nontpmr bridge neighbor #-- -- Nearest customer bridge neighbor	Chassis ID flag: • An asterisk (*) indicates the nearest non-TPMR bridge neighbor. • A pound sign (#) indicates the nearest customer bridge neighbor.

display lldp statistics

Use **display lldp statistics** to display the global LLDP statistics or the LLDP statistics of a port.

Syntax

display lldp statistics [**global** | [**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** | **nearest-nontpmr** }]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

global: Displays the global LLDP statistics.

interface *interface-type interface-number*: Specifies a port by its type and number.

agent: Specifies an LLDP agent type. If you do not specify an agent type, the command displays the statistics for all LLDP agents.

nearest-bridge: Specifies nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

Usage guidelines

If you do not specify any keywords or arguments, the command displays the global LLDP statistics and the LLDP statistics of all ports.

Examples

Display the global LLDP statistics and the LLDP statistics of all ports.

```
<Sysname> display lldp statistics
LLDP statistics global information:
LLDP neighbor information last change time:0 days, 0 hours, 4 minutes, 40 seconds
The number of LLDP neighbor information inserted : 1
The number of LLDP neighbor information deleted  : 1
The number of LLDP neighbor information dropped  : 0
The number of LLDP neighbor information aged out : 1

LLDP statistics information of port 1 [GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
```

```
The number of LLDP frames transmitted           : 0
The number of LLDP frames received              : 0
The number of LLDP frames discarded             : 0
The number of LLDP error frames                 : 0
The number of LLDP TLVs discarded               : 0
The number of LLDP TLVs unrecognized            : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted            : 0
The number of CDP frames received               : 0
The number of CDP frames discarded              : 0
The number of CDP error frames                  : 0

LLDP agent nearest-nontpmr:
The number of LLDP frames transmitted           : 0
The number of LLDP frames received              : 0
The number of LLDP frames discarded             : 0
The number of LLDP error frames                 : 0
The number of LLDP TLVs discarded               : 0
The number of LLDP TLVs unrecognized            : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted            : 0
The number of CDP frames received               : 0
The number of CDP frames discarded              : 0
The number of CDP error frames                  : 0

LLDP agent nearest-customer:
The number of LLDP frames transmitted           : 0
The number of LLDP frames received              : 0
The number of LLDP frames discarded             : 0
The number of LLDP error frames                 : 0
The number of LLDP TLVs discarded               : 0
The number of LLDP TLVs unrecognized            : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted            : 0
The number of CDP frames received               : 0
The number of CDP frames discarded              : 0
The number of CDP error frames                  : 0
```

Display the LLDP statistics for the nearest customer bridge agents on GigabitEthernet 1/0/1.

```
<Sysname> display lldp statistics interface GigabitEthernet1/0/1 agent nearest-customer
LLDP statistics information of port 1 [GigabitEthernet1/0/1]:
LLDP agent nearest-customer:
The number of LLDP frames transmitted           : 0
The number of LLDP frames received              : 0
The number of LLDP frames discarded             : 0
The number of LLDP error frames                 : 0
The number of LLDP TLVs discarded               : 0
The number of LLDP TLVs unrecognized            : 0
The number of LLDP neighbor information aged out : 0
```

```
The number of CDP frames transmitted            : 0
The number of CDP frames received               : 0
The number of CDP frames discarded              : 0
The number of CDP error frames                  : 0
```

Table 3 Command output

Field	Description
LLDP statistics global information	Global LLDP statistics.
LLDP neighbor information last change time	Time when the neighbor information was last updated.
The number of LLDP neighbor information inserted	Number of times neighbor information was added.
The number of LLDP neighbor information deleted	Number of times neighbor information was removed.
The number of LLDP neighbor information dropped	Number of times neighbor information was dropped due to lack of available memory space.

display lldp status

Use **display lldp status** to display LLDP status.

Syntax

display lldp status [**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** | **nearest-nontpmr** }]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify this option, the command displays the global LLDP status and the LLDP status of all ports.

agent: Specifies an LLDP agent type. If you do not specify an agent type, the command displays the status information for all LLDP agents.

nearest-bridge: Specifies nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

Examples

Display the global LLDP status and the LLDP status of each port.

```
<Sysname> display lldp status
Global status of LLDP: Enable
Bridge mode of LLDP: customer-bridge
The current number of LLDP neighbors: 5
The current number of CDP neighbors: 0
LLDP neighbor information last changed time: 0 days, 0 hours, 4 minutes, 40 seconds
```

```
Transmit interval              : 30s
Fast transmit interval         : 1s
Transmit max credit            : 5
Hold multiplier                : 4
Reinit delay                   : 2s
Trap interval                  : 5s
Fast start times               : 3

LLDP status information of port 1 [GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
Port status of LLDP            : Enable
Admin status                   : TX_RX
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 5
Number of MED neighbors        : 2
Number of CDP neighbors        : 0
Number of sent optional TLV    : 12
Number of received unknown TLV : 5

LLDP agent nearest-nontpmr:
Port status of LLDP            : Enable
Admin status                   : TX_RX
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 5
Number of MED neighbors        : 2
Number of CDP neighbors        : 0
Number of sent optional TLV    : 12
Number of received unknown TLV : 5

LLDP agent nearest-customer:
Port status of LLDP            : Enable
Admin status                   : TX_RX
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 5
Number of MED neighbors        : 2
Number of CDP neighbors        : 0
Number of sent optional TLV    : 12
Number of received unknown TLV : 5
```

Table 4 Command output

Field	Description
Bridge mode of LLDP	LLDP bridge mode: service-bridge or customer-bridge.

Field	Description
Global status of LLDP	Indicates whether LLDP is globally enabled.
LLDP neighbor information last changed time	Time when the neighbor information was last updated.
Transmit interval	LLDP frame transmission interval.
Hold multiplier	TTL multiplier.
Reinit delay	LLDP reinitialization delay.
Transmit max credit	Token bucket size for sending LLDP frames.
Trap interval	Trap transmission interval.
Fast start times	Number of LLDP frames sent each time fast LLDP frame transmission is triggered.
Port 1	LLDP status of port 1.
Port status of LLDP	Indicates whether LLDP is enabled on the port.
Admin status	LLDP operating mode of the port: • **TX_RX**—The port can send and receive LLDP frames. • **Rx_Only**—The port can only receive LLDP frames. • **Tx_Only**—The port can only send LLDP frames. • **Disable**—The port cannot send or receive LLDP frames.
Trap Flag	Indicates whether trapping is enabled.
Polling interval	LLDP polling interval, which is 0 when LLDP polling is disabled.
Number of neighbors	Number of LLDP neighbors connecting to the port.
Number of MED neighbors	Number of MED neighbors connecting to the port.
Number of CDP neighbors	Number of CDP neighbors connecting to the port.
Number of sent optional TLV	Number of optional TLVs contained in an LLDP frame sent through the port.
Number of received unknown TLV	Number of unknown TLVs contained in a received LLDP frame.

display lldp tlv-config

Use **display lldp tlv-config** to display the types of advertisable optional LLDP TLVs of a port.

Syntax

display lldp tlv-config [**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** | **nearest-nontpmr** }]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify this option, the command displays the types of advertisable optional TLVs of all ports.

agent: Specifies an LLDP agent type. If you do not specify an agent type, the command displays the types of advertisable optional LLDP TLVs for all LLDP agents.

nearest-bridge: Specifies nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

Examples

Display the types of advertisable optional LLDP TLVs of GigabitEthernet 1/0/1.

```
<Sysname> display lldp tlv-config interface gigabitethernet 1/0/1
LLDP tlv-config of port 1[GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
NAME                              STATUS    DEFAULT
Basic optional TLV:
 Port Description TLV             YES       YES
 System Name TLV                  YES       YES
 System Description TLV           YES       YES
 System Capabilities TLV          YES       YES
 Management Address TLV           YES       YES
IEEE 802.1 extend TLV:
 Port VLAN ID TLV                 YES       YES
 Port And Protocol VLAN ID TLV    YES       YES
 VLAN Name TLV                    YES       YES
 DCBX TLV                         NO        NO
 EVB TLV                          NO        NO
 Link Aggregation TLV             YES       YES
 Management VID TLV               YES       YES
IEEE 802.3 extend TLV:
 MAC-Physic TLV                   YES       YES
 Power via MDI TLV                YES       YES
 Maximum Frame Size TLV           YES       YES
LLDP-MED extend TLV:
 Capabilities TLV                 YES        YES
 Network Policy TLV               YES        YES
 Location Identification TLV      NO         NO
 Extended Power via MDI TLV       YES        YES
 Inventory TLV                    YES        YES
LLDP agent nearest-nontpmr:
NAME                              STATUS    DEFAULT
Basic optional TLV:
 Port Description TLV             YES       NO
 System Name TLV                  YES       NO
 System Description TLV           YES       NO
 System Capabilities TLV          YES       NO
 Management Address TLV           YES       NO
```

```
IEEE 802.1 extend TLV:
 Port VLAN ID TLV                 YES       NO
 Port And Protocol VLAN ID TLV    YES       NO
 VLAN Name TLV                    YES       NO
 DCBX TLV                         NO        NO
 EVB TLV                          YES       YES
 Link Aggregation TLV             YES       NO
 Management VID TLV               NO        NO
IEEE 802.3 extend TLV:
 MAC-Physic TLV                   YES       NO
 Power via MDI TLV                YES       NO
 Maximum Frame Size TLV           YES       NO
LLDP-MED extend TLV:
 Capabilities TLV                 YES        NO
 Network Policy TLV               YES        NO
 Location Identification TLV      NO         NO
 Extended Power via MDI TLV       YES        NO
 Inventory TLV                    YES        NO

LLDP agent nearest-customer:
NAME                              STATUS    DEFAULT
Basic optional TLV:
 Port Description TLV             YES       YES
 System Name TLV                  YES       YES
 System Description TLV           YES       YES
 System Capabilities TLV          YES       YES
 Management Address TLV           YES       YES
IEEE 802.1 extend TLV:
 Port VLAN ID TLV                 YES       YES
 Port And Protocol VLAN ID TLV    YES       YES
 VLAN Name TLV                    YES       YES
 DCBX TLV                         NO        NO
 EVB TLV                          NO        NO
 Link Aggregation TLV             YES       NO
 Management VID TLV               YES       YES
IEEE 802.3 extend TLV:
 MAC-Physic TLV                   YES       NO
 Power via MDI TLV                YES       NO
 Maximum Frame Size TLV           YES       NO
LLDP-MED extend TLV:
 Capabilities TLV                 YES        YES
 Network Policy TLV               YES        YES
 Location Identification TLV      NO         NO
 Extended Power via MDI TLV       YES        NO
 Inventory TLV                    YES        YES
```

Table 5 Command output

Field	Description
LLDP tlv-config of port 1	Advertisable optional TLVs of port 1.
NAME	TLV type.
STATUS	Indicates whether the type of TLV is sent through a port.
DEFAULT	Indicates whether the type of TLV is sent through a port by default.
Basic optional TLV	Basic optional TLVs: • Port Description TLV. • System Name TLV. • System Description TLV. • System Capabilities TLV. • Management Address TLV.
IEEE 802.1 extended TLV	IEEE 802.1 organizationally specific TLVs: • Port PVID TLV. • Port and protocol VLAN ID TLV. • VLAN name TLV. • DCBX TLV. DCBX TLVs are not supported in the current software version. • EVB TLV. EVB TLVs are not supported in the current software version. • Management VID TLV.
IEEE 802.3 extended TLV	IEEE 802.3 organizationally specific TLVs: • MAC-Physic TLV. • Power via MDI TLV. • Link aggregation TLV. • Maximum frame size TLV.
LLDP-MED extend TLV	LLDP-MED TLVs: • Capabilities TLV. • Network Policy TLV. • Extended Power-via-MDI TLV. • Location Identification TLV. • Inventory TLV.
Inventory TLV	Inventory TLVs: • Hardware Revision TLV. • Firmware Revision TLV. • Software Revision TLV. • Serial Number TLV. • Manufacturer Name TLV. • Model name TLV. • Asset ID TLV.

lldp admin-status

Use **lldp admin-status** to set the LLDP operating mode.

Use **undo lldp admin-status** to restore the default.

Syntax

In Layer 2 Ethernet interface view or management Ethernet interface view:

lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **admin-status** { **disable** | **rx** | **tx** | **txrx** }

undo lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **admin-status**

In Layer 2 aggregate interface view:

lldp agent { **nearest-customer** | **nearest-nontpmr** } **admin-status** { **disable** | **rx** | **tx** | **txrx** }

undo lldp agent { **nearest-customer** | **nearest-nontpmr** } **admin-status**

Default

The nearest bridge agent operates in **TxRx** mode, and the nearest customer bridge agent and nearest non-TPMR bridge agent operate in **Disable** mode.

Views

Layer 2 Ethernet interface view

Management Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

agent: Specifies an LLDP agent type. If you do not specify an agent type in Ethernet or management Ethernet interface view, the command sets the operating mode for nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

disable: Specifies the **Disable** mode. A port in this mode cannot send or receive LLDP frames.

rx: Specifies the **Rx** mode. A port in this mode can only receive LLDP frames.

tx: Specifies the **Tx** mode. A port in this mode can only send LLDP frames.

txrx: Specifies the **TxRx** mode. A port in this mode can send and receive LLDP frames.

Examples

Set the LLDP operating mode to **Rx** for the nearest customer bridge agents on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp agent nearest-customer admin-status rx
```

lldp check-change-interval

Use **lldp check-change-interval** to enable LLDP polling and set the polling interval.

Use **undo lldp check-change-interval** to disable LLDP polling.

Syntax

In Layer 2 Ethernet interface view or management Ethernet interface view:

lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **check-change-interval** *interval*

undo lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **check-change-interval**

In Layer 2 aggregate interface view:

lldp agent { **nearest-customer** | **nearest-nontpmr** } **check-change-interval** *interval*

undo lldp agent { **nearest-customer** | **nearest-nontpmr** } **check-change-interval**

Default

LLDP polling is disabled.

Views

Layer 2 Ethernet interface view

Management Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

agent: Specifies an LLDP agent type. If you do not specify an agent type in Ethernet or management Ethernet interface view, the command enables LLDP polling and sets the polling interval for nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

interval: Sets the LLDP polling interval in the range of 1 to 30 seconds.

Examples

Enable LLDP polling and set the polling interval to 30 seconds for the nearest customer bridge agents on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp agent nearest-customer check-change-interval 30
```

lldp compliance admin-status cdp

Use **lldp compliance admin-status cdp** to set the operating mode of CDP-compatible LLDP.

Use **undo lldp compliance admin-status cdp** to restore the default.

Syntax

lldp compliance admin-status cdp { **disable** | **rx** | **txrx** }

undo lldp compliance admin-status cdp

Default

CDP-compatible LLDP operates in **Disable** mode.

Views

Layer 2 Ethernet interface view

Management Ethernet interface view

Predefined user roles

network-admin

Parameters

`disable`: Specifies the **Disable** mode. CDP-compatible LLDP in this mode cannot receive or transmit CDP packets.

`txrx`: Specifies the **TxRx** mode. CDP-compatible LLDP in this mode can send and receive CDP packets.

`rx`: Specifies the **Rx** mode. CDP-compatible LLDP in this mode can receive but cannot send CDP packets.

Usage guidelines

For your device to work with Cisco IP phones, you must perform the following tasks:

- Enable CDP-compatible LLDP globally.
- Configure CDP-compatible LLDP to operate in TxRx mode on the specified ports.

Examples

Enable CDP-compatible LLDP globally and configure CDP-compatible LLDP to operate in **TxRx** mode on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] lldp compliance cdp
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp compliance admin-status cdp txrx
```

Related commands

`lldp compliance cdp`

lldp compliance cdp

Use **`lldp compliance cdp`** to enable CDP compatibility.

Use **`undo lldp compliance cdp`** to disable CDP compatibility.

Syntax

`lldp compliance cdp`

`undo lldp compliance cdp`

Default

CDP compatibility is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The maximum TTL that CDP allows is 255 seconds. To make CDP-compatible LLDP work correctly with Cisco IP phones, set the LLDP frame transmission interval to be no more than 1/3 of the TTL value.

Examples

Enable CDP compatibility.

```
<Sysname> system-view
[Sysname] lldp compliance cdp
```

Related commands

lldp hold-multiplier

lldp timer tx-interval

lldp enable

Use **lldp enable** to enable LLDP on a port.

Use **undo lldp enable** to disable LLDP on a port.

Syntax

lldp enable

undo lldp enable

Default

LLDP is enabled on a port.

Views

Layer 2 Ethernet interface view

Management Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

LLDP takes effect on a port only when LLDP is enabled both globally and on the port.

Examples

Disable LLDP on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo lldp enable
```

Related commands

lldp global enable

lldp encapsulation snap

Use **lldp encapsulation snap** to set the encapsulation format for LLDP frames to SNAP.

Use **undo lldp encapsulation** to restore the default.

Syntax

In Layer 2 Ethernet interface view or management Ethernet interface view:

lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **encapsulation snap**

undo lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **encapsulation**

In Layer 2 aggregate interface view:

lldp agent { **nearest-customer** | **nearest-nontpmr** } **encapsulation snap**

undo lldp agent { **nearest-customer** | **nearest-nontpmr** } **encapsulation**

Default

The encapsulation format for LLDP frames is Ethernet II.

Views

Layer 2 Ethernet interface view

Management Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

agent: Specifies an LLDP agent type. If you do not specify an agent type in Ethernet or management Ethernet interface view, the command sets the LLDP frame encapsulation format for nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

Usage guidelines

LLDP-CDP packets use only SNAP encapsulation.

Examples

Set the encapsulation format for LLDP frames to SNAP on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp encapsulation snap
```

lldp fast-count

Use **lldp fast-count** to set the number of LLDP frames sent each time fast LLDP frame transmission is triggered.

Use **undo lldp fast-count** to restore the default.

Syntax

lldp fast-count *count*

undo lldp fast-count

Default

Four LLDP frames are sent each time fast LLDP frame transmission is triggered.

Views

System view

Predefined user roles

network-admin

Parameters

count: Sets the number of LLDP frames sent each time fast LLDP frame transmission is triggered. The value range is 1 to 8.

Examples

Configure the device to send five LLDP frames each time fast LLDP frame transmission is triggered.

```
<Sysname> system-view
[Sysname] lldp fast-count 5
```

lldp global enable

Use **lldp global enable** to enable LLDP globally.

Use **undo lldp global enable** to disable LLDP globally.

Syntax

lldp global enable

undo lldp global enable

Default

If the device starts up with the initial configuration, LLDP is disabled globally.

If the device starts up with the factory defaults, LLDP is enabled globally.

For more information about device startup with the initial configuration or factory defaults, see *Fundamentals Configuration Guide*.

Views

System view

Predefined user roles

network-admin

Usage guidelines

LLDP takes effect on a port only when LLDP is enabled both globally and on the port.

Examples

Disable LLDP globally.

```
<Sysname> system-view
[Sysname] undo lldp global enable
```

Related commands

lldp enable

lldp global tlv-config basic-tlv port-id

Use **lldp global tlv-config basic-tlv port-id** to set the type of port ID TLVs advertised by LLDP globally.

Use **undo lldp global tlv-config basic-tlv port-id** to restore the default.

NOTE:

This command is supported only in Release 6331 and later.

Syntax

lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **global tlv-config basic-tlv port-id** *type-id*

undo lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **global tlv-config basic-tlv port-id**

Default

An interface advertises port ID TLVs that contain interface MAC addresses if it receives LLDP-MED TLVs and advertises port ID TLVs that contain interface names if no LLDP-MED TLVs are received.

Views

System view

Predefined user roles

network-admin

Parameters

agent: Specifies an LLDP agent type. If you do not specify an agent type, the command sets the port ID TLV type for nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

type-id: Specifies a port ID TLV type. The available value is 5, which represents that port ID TLVs contain interface names.

Usage guidelines

This command enables the device to advertise only port ID TLVs that contain interface names. Execute this command if LLDP neighbors must obtain interface names from LLDPDUs.

You can configure the port ID TLV type in system view or interface view. The interface-specific setting takes precedence over the global setting.

Examples

Enable the device to advertise port ID TLVs that contain interface names.

```
<Sysname> system-view
[Sysname] lldp global tlv-config basic-tlv port-id 5
```

Related commands

lldp tlv-config basic-tlv port-id

lldp global tlv-enable basic-tlv management-address-tlv

Use **lldp global tlv-enable basic-tlv management-address-tlv** to enable advertisement of the management address TLV globally and set the management address to be advertised.

Use **undo lldp global tlv-enable basic-tlv management-address-tlv** to restore the default.

Syntax

lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **global tlv-enable basic-tlv management-address-tlv** [**ipv6**] { *ip-address* | **interface loopback** *interface-number* | **interface m-gigabitethernet** *interface-number* | **interface vlan-interface** *interface-number* }

undo lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **global tlv-enable basic-tlv management-address-tlv**

Default

Advertisement of the management address TLV is disabled globally.

Views

System view

Predefined user roles

network-admin

Parameters

agent: Specifies an LLDP agent type. If you do not specify an agent type, this command applies to the nearest bridge agent.

- **nearest-customer**: Specifies the nearest customer bridge agent.
- **nearest-nontpmr**: Specifies the nearest non-TPMR bridge agent.

ipv6: Specifies an IPv6 management address. If you do not specify this keyword, an IPv4 management address will be advertised.

ip-address: Specifies the management address to be advertised.

interface loopback *interface-number*: Specifies a loopback interface by its number in the range of 0 to 127. The IP address of the loopback interface will be advertised as the management address. The value range for the *interface-number* argument is 0 to 127.

interface m-gigabitethernet *interface-number*: Specifies an M-GigabitEthernet interface by is number. The IP address of the M-GigabitEthernet interface will be advertised as the management address.

interface vlan-interface *interface-number*: Specifies a VLAN interface by is number in the range of 1 to 4094. The IP address of the VLAN interface will be advertised as the management address.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

You can configure advertisement of the management address TLV globally or on a per-interface basis. The device selects the management address TLV advertisement setting for an interface in the following order:

1. Interface-based setting, configured by using the **lldp tlv-enable** command with the **management-address-tlv** keyword.
2. Global setting, configured by using the **lldp global tlv-enable basic-tlv management-address-tlv** command.
3. Default setting for the interface.

   By default:

   - The nearest bridge agent and nearest customer bridge agent advertise the management address TLV.
   - The nearest non-TPMR bridge agent does not advertise the management address TLV.

The IPv4 or IPv6 address of the LLDP frame sending port will be advertised as the management address when the following conditions exist:

- The *ip-address* argument is not configured.
- The specified loopback interface, M-GigabitEthernet interface, or VLAN interface does not have an IPv4 or IPv6 address, or the specified interface does not exist.

If the LLDP frame sending port does not have an IPv4 or IPv6 address, the MAC address of the port will be advertised.

If you specify the **ipv6** keyword, the management address is the IPv6 address. If you do not specify the **ipv6** keyword, the management address is the IPv4 address.

Examples

Enable advertisement of the management address TLV globally and set the advertised management address to 192.168.1.1.

```
<Sysname> system-view
[Sysname] lldp agent nearest-customer global tlv-enable basic-tlv management-address-tlv
192.168.1.1
```

Related commands

lldp tlv-enable

lldp hold-multiplier

Use **lldp hold-multiplier** to set the TTL multiplier.

Use **undo lldp hold-multiplier to** restore the default.

Syntax

lldp hold-multiplier *value*

undo lldp hold-multiplier

Default

The TTL multiplier is 4.

Views

System view

Predefined user roles

network-admin

Parameters

value: Sets the TTL multiplier in the range of 2 to 10.

Usage guidelines

The TTL TLV carried in an LLDPDU determines how long the device information carried in the LLDPDU can be saved on a recipient device.

By setting the TTL multiplier, you can set the TTL of locally sent LLDP frames. The TTL is expressed by using the following formula:

TTL = Min (65535, (TTL multiplier × LLDP frame transmission interval + 1))

As the expression shows, the TTL can be up to 65535 seconds.

Examples

Set the TTL multiplier to 6.

```
<Sysname> system-view
[Sysname] lldp hold-multiplier 6
```

Related commands

lldp timer tx-interval

lldp ignore-pvid-inconsistency

Use **lldp ignore-pvid-inconsistency** to disable LLDP PVID inconsistency check.

Use **undo lldp ignore-pvid-inconsistency** to enable LLDP PVID inconsistency check.

Syntax

lldp ignore-pvid-inconsistency

undo lldp ignore-pvid-inconsistency

Default

LLDP PVID inconsistency check is enabled.

Views

System view

Default command level

network-admin

Usage guidelines

By default, when the system receives an LLDP packet, it compares the PVID value contained in packet with the PVID configured on the receiving interface. If the two PVIDs do not match, a log message will be printed to notify the user.

You can disable PVID inconsistency check if different PVIDs are required on a link.

Examples

Disable LLDP PVID inconsistency check.

```
<Sysname> system-view
[Sysname] lldp ignore-pvid-inconsistency
```

lldp local-information all-interface

Use **lldp local-information all-interface** to enable displaying LLDP local information about all interfaces.

Use **undo lldp local-information all-interface** to disable displaying LLDP local information about interfaces not in physically up state.

NOTE:

This command is supported only in Release 6331 and later.

Syntax

lldp local-information all-interface

undo lldp local-information all-interface

Default

The **display lldp local-information** command displays information about physically up interfaces.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command enables the **display lldp local-information** command to display LLDP local information about all interfaces.

By default, the **display lldp local-information** command displays information about physically up interfaces. The media devices from some vendors can obtain interface information from H3C devices only through LLDP. For the media devices to obtain all interface information, enable the **display lldp local-information** command to display LLDP local information about all interfaces.

Examples

Enable displaying LLDP local information about all interfaces.

```
<Sysname> system-view
[Sysname] lldp local-information all-interface
```

Related commands

display lldp local-information

lldp management-address

Use **lldp management-address** to enable the device to generate an ARP or ND entry after receiving an LLDP frame that carries a management address TLV.

Use **undo lldp management-address** to restore the default.

Syntax

In Layer 2 Ethernet interface view:

lldp management-address { **arp-learning** | **nd-learning** } **vlan** *vlan-id*

undo lldp management-address { **arp-learning** | **nd-learning** }

Default

The device does not generate an ARP or ND entry after receiving an LLDP frame that carries a management address TLV.

Views

Layer 2 Ethernet interface view

Default command level

network-admin

Parameters

arp-learning: Generates an ARP entry if the received management address TLV contains an IPv4 address.

nd-learning: Generates an ND entry if the received management address TLV contains an IPv6 address.

vlan *vlan-id*: Specifies the ID of the VLAN to which the generated ARP or ND entry belongs. The value range for the VLAN ID is 1 to 4094.

Usage guidelines

You can enable the device to generate both ARP entries and ND entries.

In Layer 2 Ethernet interface view, after you execute this command, the Layer 2 Ethernet interface is recorded as the output interface in the generated entries. The VLAN to which the entries belong is the VLAN specified by this command. The device cannot generate ARP or ND entries in one of the following situations:

- The specified VLAN or the corresponding VLAN interface does not exist.
- The VLAN interface to which the VLAN ID belongs is physically down.

In Layer 2 Ethernet interface view, this command must be configured together with the **lldp source-mac vlan** command. The **lldp source-mac vlan** command enables the Layer 2 Ethernet interface to use the MAC address of a VLAN interface instead of its own MAC address as the source MAC address of LLDP frames. This ensures that the LLDP neighbor can learn correct ARP or ND entries.

Examples

Configure GigabitEthernet 1/0/1 to generate an ARP entry after receiving an LLDP frame carrying an IPv4 management address TLV.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp management-address arp-learning
```

Related commands

lldp source-mac vlan

lldp management-address-format string

Use **lldp management-address-format string** to set the encoding format of the management address to string.

Use **undo lldp management-address-format** to restore the default.

Syntax

In Layer 2 Ethernet interface view/management Ethernet interface view:

lldp [agent { nearest-customer | nearest-nontpmr }] management-address-format string

undo lldp [agent { nearest-customer | nearest-nontpmr }] management-address-format

In Layer 2 aggregate interface view:

lldp agent { nearest-customer | nearest-nontpmr } management-address-format string

undo lldp agent { nearest-customer | nearest-nontpmr } management-address-format

Default

The encoding format of the management address is numeric.

Views

Layer 2 Ethernet interface view

Management Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

agent: Specifies an LLDP agent type. If you do not specify an agent type in Ethernet or management Ethernet interface view, the command sets the encoding format of the management address for nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

Usage guidelines

LLDP neighbors must use the same encoding format for the management address.

The device supports only the numeric encoding format for IPv6 management addresses.

Examples

Set the encoding format of the management address to string for the nearest customer bridge agents on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp agent nearest-customer management-address-format
string
```

lldp max-credit

Use **lldp max-credit** to set the token bucket size for sending LLDP frames.

Use **undo lldp max-credit** to restore the default.

Syntax

lldp max-credit *credit-value*

undo lldp max-credit

Default

The token bucket size for sending LLDP frames is 5.

Views

System view

Predefined user roles

network-admin

Parameters

credit-value: Specifies the token bucket size for sending LLDP frames, in the range of 1 to 100.

Examples

Set the token bucket size for sending LLDP frames to 10.

```
<Sysname> system-view
[Sysname] lldp max-credit 10
```

lldp mode

Use **lldp mode** to configure LLDP to operate in service bridge mode.

Use **undo lldp mode** to restore the default.

Syntax

lldp mode service-bridge

undo lldp mode

Default

LLDP operates in customer bridge mode.

Views

System view

Predefined user roles

network-admin

Parameters

service-bridge: Specifies the service bridge mode.

Usage guidelines

The LLDP agent types supported by LLDP depend on the LLDP bridge mode:

- **Service bridge mode**—LLDP supports nearest bridge agents and nearest non-TPMR bridge agents. LLDP processes the LLDP frames with destination MAC addresses for these agents and transparently transmits the LLDP frames with other destination MAC addresses in a VLAN.
- **Customer bridge mode**—LLDP supports nearest bridge agents, nearest non-TPMR bridge agents, and nearest customer bridge agents. LLDP processes the LLDP frames with destination MAC addresses for these agents and transparently transmits the LLDP frames with other destination MAC addresses in a VLAN.

The bridge mode configuration takes effect only when LLDP is enabled globally. If LLDP is disabled globally, LLDP can only operate in customer bridge mode.

Examples

Configure LLDP to operate in service bridge mode.

```
<Sysname> system-view
[Sysname] lldp mode service-bridge
```

Related commands

lldp global enable

lldp notification med-topology-change enable

Use **lldp notification med-topology-change enable** to enable LLDP-MED trapping.

Use **undo lldp notification med-topology-change enable** to disable LLDP-MED trapping.

Syntax

lldp notification med-topology-change enable

undo lldp notification med-topology-change enable

Default

LLDP-MED trapping is disabled.

Views

Layer 2 Ethernet interface view

Management Ethernet interface view

Predefined user roles

network-admin

Examples

Enable LLDP-MED trapping on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp notification med-topology-change enable
```

lldp notification remote-change enable

Use **lldp notification remote-change enable** to enable LLDP trapping.

Use **undo lldp notification remote-change enable** to disable LLDP trapping.

Syntax

In Layer 2 Ethernet interface view/management Ethernet interface view:

lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **notification remote-change enable**

undo lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **notification remote-change enable**

In Layer 2 aggregate interface view:

lldp agent { **nearest-customer** | **nearest-nontpmr** } **notification remote-change enable**

undo lldp agent { **nearest-customer** | **nearest-nontpmr** } **notification remote-change enable**

Default

LLDP trapping is disabled.

Views

Layer 2 Ethernet interface view

Management Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

agent: Specifies an LLDP agent type. If you do not specify an agent type in Ethernet or management Ethernet interface view, the command enables LLDP trapping for nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

Examples

Enable LLDP trapping for the nearest customer bridge agent on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp agent nearest-customer notification remote-change
enable
```

lldp source-mac vlan

Use **lldp source-mac vlan** to set the source MAC address of LLDP frames to the MAC address of a VLAN interface.

Use **undo lldp source-mac vlan** to restore the default.

Syntax

lldp source-mac vlan *vlan-id*

undo lldp source-mac vlan

Default

The source MAC address of LLDP frames is the MAC address of the interface.

Views

Layer 2 Ethernet interface view

Default command level

network-admin

Parameters

vlan *vlan-id*: Specifies a VLAN ID in the range of 1 to 4094. The MAC address of the VLAN interface will be used as the source MAC address of outgoing LLDP frames.

Usage guidelines

In Layer 2 Ethernet interface view, this command must be configured together with the **lldp management-address arp-learning** command to ensure that the LLDP neighbor can learn correct ARP or ND entries.

In Layer 2 Ethernet interface view, the source MAC address of outgoing LLDP frames is the MAC address of a VLAN interface to which the specified VLAN ID belongs. The source MAC address of outgoing LLDP frames is the MAC address of the Layer 2 Ethernet interface in the following situations:

- The specified VLAN or the corresponding VLAN interface does not exist.
- The VLAN interface to which the VLAN ID belongs is physically down.

Examples

Set the source MAC address of LLDP frames to the MAC address of VLAN-interface 4094.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp source-mac vlan 4094
```

Related commands

lldp management-address arp-learning

lldp timer fast-interval

Use **lldp timer fast-interval** to set an interval for fast LLDP frame transmission.

Use **undo lldp timer fast-interval** to restore the default.

Syntax

lldp timer fast-interval *interval*

undo lldp timer fast-interval

Default

The interval for fast LLDP frame transmission is 1 second.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Sets an interval for fast LLDP frame transmission, in the range of 1 to 3600 seconds.

Examples

Set the interval for fast LLDP frame transmission to 2 seconds.

```
<Sysname> system-view
[Sysname] lldp timer fast-interval 2
```

lldp timer notification-interval

Use **lldp timer notification-interval** to set the LLDP trap and LLDP-MED trap transmission interval.

Use **undo lldp timer notification-interval** to restore the default.

Syntax

lldp timer notification-interval *interval*

undo lldp timer notification-interval

Default

The LLDP trap and LLDP-MED trap transmission interval is 30 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Sets the LLDP trap and LLDP-MED trap transmission interval in the range of 5 to 3600 seconds.

Examples

Set both the LLDP trap and LLDP-MED trap transmission interval to 8 seconds.

```
<Sysname> system-view
```

```
[Sysname] lldp timer notification-interval 8
```

lldp timer reinit-delay

Use **lldp timer reinit-delay** to set the LLDP reinitialization delay.

Use **undo lldp timer reinit-delay** to restore the default.

Syntax

lldp timer reinit-delay *delay*

undo lldp timer reinit-delay

Default

The LLDP reinitialization delay is 2 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

delay: Sets the LLDP reinitialization delay in the range of 1 to 10 seconds.

Examples

Set the LLDP reinitialization delay to 4 seconds.

```
<Sysname> system-view
[Sysname] lldp timer reinit-delay 4
```

lldp timer tx-interval

Use **lldp timer tx-interval** to set the LLDP frame transmission interval.

Use **undo lldp timer tx-interval** to restore the default.

Syntax

lldp timer tx-interval *interval*

undo lldp timer tx-interval

Default

The LLDP frame transmission interval is 30 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Sets the LLDP frame transmission interval in the range of 1 to 32768 seconds.

Examples

Set the LLDP frame transmission interval to 20 seconds.

```
<Sysname> system-view
```

```
[Sysname] lldp timer tx-interval 20
```

lldp tlv-config basic-tlv port-id

Use **lldp tlv-config basic-tlv port-id** to set the type of port ID TLVs advertised by LLDP on an interface.

Use **undo lldp tlv-config basic-tlv port-id** to restore the default.

NOTE:

This command is supported only in Release 6331 and later.

Syntax

In Layer 2 Ethernet interface view or management Ethernet interface view:

lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **tlv-config basic-tlv port-id** *type-id*

undo lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **tlv-config basic-tlv port-id**

In Layer 2 aggregate interface view:

lldp agent { **nearest-customer** | **nearest-nontpmr** } **tlv-config basic-tlv port-id** *type-id*

undo lldp agent { **nearest-customer** | **nearest-nontpmr** } **tlv-config basic-tlv port-id**

Default

An interface advertises port ID TLVs that contain interface MAC addresses if it receives LLDP-MED TLVs and advertises port ID TLVs that contain interface names if no LLDP-MED TLVs are received.

Views

Layer 2 Ethernet interface view

Management Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

agent: Specifies an LLDP agent type. If you do not specify an agent type, the command sets the port ID TLV type for nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

type-id: Specifies a port ID TLV type. The available value is 5, which represents that port ID TLVs contain interface names.

Usage guidelines

This command enables an interface to advertise only port ID TLVs that contain interface names. Execute this command if LLDP neighbors must obtain interface names from LLDPDUs.

You can configure the port ID TLV type in system view or interface view. The interface-specific setting takes precedence over the global setting.

Examples

Enable GigabitEthernet 1/0/1 to advertise port ID TLVs that contain interface names.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp tlv-config basic-tlv port-id 5
```

Related commands

lldp global tlv-config basic-tlv port-id

lldp tlv-enable

Use **lldp tlv-enable** to configure the types of advertisable TLVs on a port.

Use **undo lldp tlv-enable** to disable the advertising of the specified types of TLVs on a port.

Syntax

In Layer 2 Ethernet interface view:

- For nearest bridge agents:

  lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address* | **interface loopback** *interface-number*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** | **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] } | **dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **network-policy** [*vlan-id*] | **power-over-ethernet** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } } }

  undo lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address* | **interface loopback** *interface-number*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** | **protocol-vlan-id** | **vlan-name** | **management-vid** } | **dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **network-policy** [*vlan-id*] | **power-over-ethernet** | **location-id** } }

- For nearest non-TPMR bridge agents:

  lldp agent nearest-nontpmr tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** } }

  lldp tlv-enable dot1-tlv { **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] }

  undo lldp agent nearest-nontpmr tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** } }

  undo lldp tlv-enable dot1-tlv { **protocol-vlan-id** | **vlan-name** | **management-vid** }

- For nearest customer bridge agents:

lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** } }

lldp tlv-enable dot1-tlv { **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] }

undo lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** } }

undo lldp tlv-enable dot1-tlv { **protocol-vlan-id** | **vlan-name** | **management-vid** }

In management Ethernet interface view:

lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **power-over-ethernet** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } } }

lldp agent { **nearest-nontpmr** | **nearest-customer** } **tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** } }

undo lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **power-over-ethernet** | **location-id** } }

undo lldp agent { **nearest-nontpmr** | **nearest-customer** } **tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** } }

In Layer 2 aggregate interface view:

lldp agent nearest-nontpmr tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

lldp tlv-enable dot1-tlv { **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] }

undo lldp agent nearest-nontpmr tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address*] | **port-description** |

system-capability | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

undo lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

undo lldp tlv-enable dot1-tlv { **protocol-vlan-id** | **vlan-name** | **management-vid** }

Default

On Layer 2 Ethernet interfaces:

- Nearest bridge agents can advertise all types of LLDP TLVs except the following types:
  - Location identification TLVs.
  - Port and protocol VLAN ID TLVs.
  - VLAN name TLVs.
  - Management VLAN ID TLVs.
- Nearest non-TPMR bridge agents do not advertise any TLVs.
- Nearest customer bridge agents can advertise basic TLVs and IEEE 802.1 organizationally specific TLVs.

On management Ethernet interfaces:

- Nearest bridge agents can advertise all types of LLDP TLVs except network policy TLVs. Among all the 802.1 organizationally specific TLVs, only the link aggregation TLV is supported.
- Nearest non-TPMR bridge agents do not advertise any TLVs.
- Nearest customer bridge agents can advertise basic TLVs and IEEE 802.1 organizationally specific TLVs (only link aggregation TLV is supported).

On Layer 2 aggregate interfaces:

- Nearest non-TPMR bridge agents do not advertise any TLVs.
- Nearest customer bridge agents can advertise basic TLVs and IEEE 802.1 organizationally specific TLVs. Among the IEEE 802.1 organizationally specific TLVs, only port and protocol VLAN ID TLVs, VLAN name TLVs, and management VLAN ID TLVs are supported.

Views

Layer 2 Ethernet interface view

Management Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

agent: Specifies an LLDP agent type. If you do not specify an agent type in Ethernet or management Ethernet interface view, the command configures the types of advertisable TLVs for nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

all: Advertises all TLVs of the specified type. This keyword enables the interface to advertise following TLVs:

- All basic LLDP TLVs if the **all** keyword is specified for **basic-tlv**.

- All IEEE 802.1 organizationally specific LLDP TLVs if the **all** keyword is specified for **dot1-tlv**.
- All IEEE 802.3 organizationally specific LLDP TLVs if the **all** keyword is specified for **dot3-tlv**.
- All LLDP-MED TLVs except location identification TLVs if the **all** keyword is specified for **med-tlv**.

basic-tlv: Advertises basic LLDP TLVs.

management-address-tlv [**ipv6**] [*ip-address* | **interface loopback** *interface-number*]: Advertises management address TLVs. The **ipv6** keyword indicates that the management address to be advertised is in IPv6 format. The *ip-address* argument specifies the management address to be advertised. The **interface loopback** *interface-number* option specifies the management address as the IP address of a loopback interface specified by its number. By default, the following rules apply:

- When you execute the **lldp tlv-enable** command:
  - For a Layer 2 Ethernet interface, the IPv4 or IPv6 address of a VLAN interface will be advertised as the management address when one of the following conditions exists:
    - Both the *ip-address* argument and the **interface loopback** *interface-number* option are not configured.
    - The specified loopback interface does not have an IPv4 or IPv6 address, or the specified loopback interface does not exist.

    The VLAN interface belongs to a VLAN that meets the following requirements:
    - In up state.
    - The corresponding VLAN ID is the lowest among the VLANs permitted on the interface.

    If you specify the **ipv6** keyword, the IPv6 address of the VLAN interface will be advertised. If you do not specify the **ipv6** keyword, both the IPv4 and IPv6 addresses of the VLAN interface will be advertised.

    If none of the VLAN interfaces of the permitted VLANs is assigned an IPv4 or IPv6 address or all VLAN interfaces are down, the MAC address of the interface will be advertised.
  - For a Layer 2 aggregate interface, the IPv4 or IPv6 address of a VLAN interface will be advertised as the management address if the *ip-address* argument is not configured.

    The VLAN interface belongs to a VLAN that meets the following requirements:
    - In up state.
    - The corresponding VLAN ID is the lowest among the VLANs permitted on the interface.

    If you specify the **ipv6** keyword, the IPv6 address of the VLAN interface will be advertised. If you do not specify the **ipv6** keyword, both the IPv4 and IPv6 addresses of the VLAN interface will be advertised.

    If none of the VLAN interfaces of the permitted VLANs is assigned an IPv4 or IPv6 address or all VLAN interfaces are down, the MAC address of the interface will be advertised.
  - For a management Ethernet interface, the IPv4 or IPv6 address of the interface will be advertised when the *ip-address* argument is not configured.

    If you specify the **ipv6** keyword, the IPv6 address of the interface will be advertised. If you do not specify the **ipv6** keyword, both the IPv4 and IPv6 addresses of the interface will be advertised.

    If the interface does not have an IPv4 or IPv6 address, the MAC address of the interface will be advertised.
- When you execute the **undo lldp tlv-enable** command for a Layer 2 Ethernet interface, Layer 2 aggregate interface, or management Ethernet interface:

- If you do not specify *ip-address*, **ipv6**, or **interface loopback** *interface-number*, the interface does not advertise any management address TLVs.
- If you specify *ip-address*, **ipv6**, or **interface loopback** *interface-number*, the interface advertises the default management address TLVs.

port-description: Advertises port description TLVs.

system-capability: Advertises system capabilities TLVs.

system-description: Advertises system description TLVs.

system-name: Advertises system name TLVs.

dot1-tlv: Advertises IEEE 802.1 organizationally specific LLDP TLVs.

port-vlan-id: Advertises port PVID TLVs.

protocol-vlan-id [*vlan-id*]: Advertises port and protocol VLAN ID TLVs. The *vlan-id* argument specifies a VLAN ID in the TLVs to be advertised. The VLAN ID is in the range of 1 to 4094, and the default is the lowest VLAN ID on the port.

vlan-name [*vlan-id*]: Advertises VLAN name TLVs. The *vlan-id* argument specifies a VLAN ID in the TLVs to be advertised. The VLAN ID is in the range of 1 to 4094, and the default is the lowest VLAN ID on the port. If you do not specify a VLAN ID and the port is not assigned to any VLAN, the PVID of the port is advertised.

management-vid [*mvlan-id*]: Advertises management VLAN ID TLVs. The m*vlan-id* argument specifies a management VLAN ID in the TLVs to be advertised. The management VLAN ID is in the range of 1 to 4094. If you do not specify this option, the value 0 is advertised, which means that the LLDP agent is not configured with a management VLAN ID.

link-aggregation: Advertises link aggregation TLVs.

dot3-tlv: Advertises IEEE 802.3 organizationally specific LLDP TLVs.

mac-physic: Advertises MAC/PHY configuration/status TLVs.

max-frame-size: Advertises maximum frame size TLVs.

power: Advertises power in MDI TLVs and power stateful control TLVs.

med-tlv: Advertises LLDP-MED TLVs.

capability: Advertises LLDP-MED capabilities TLVs.

inventory: Advertises the following TLVs: hardware revision, firmware revision, software revision, serial number, manufacturer name, model name, and asset ID.

location-id: Advertises location identification TLVs.

civic-address: Inserts the typical address information about the network device in location identification TLVs .

device-type: Sets a device type value in the range of 0 to 2:

- Value 0 specifies a DHCP server.
- Value 1 specifies a network device.
- Value 2 specifies an LLDP-MED endpoint.

country-code: Sets a country code defined in ISO 3166.

{ *ca-type ca-value* }&<1-10>: Configures address information. *ca-type* represents the address information type in the range of 0 to 255. *ca-value* represents address information, a string of 1 to 250 characters. &<1-10> indicates that you can specify up to 10 *ca-type ca-value* pairs.

elin-address: Inserts telephone numbers for emergencies in location identification TLVs.

tel-number: Sets the telephone number for emergencies, a string of 10 to 25 characters.

network-policy [*vlan-id*]: Advertises network policy TLVs. The *vlan-id* argument specifies the voice VLAN ID to be advertised, in the range of 1 to 4094. This option is not available on the S5110V2-SI, S5000V3-EI, S5000V5-EI, S5000E-X, S5000X-EI, or WAS6000 switch series.

power-over-ethernet: Advertises extended power-via-MDI TLVs.

Usage guidelines

Nearest bridge agents are not supported on aggregate interfaces.

You can enable the device to advertise multiple types of TLVs by using this command without the **all** keyword specified.

If the MAC/PHY configuration/status TLV is not advertisable, none of the LLDP-MED TLVs will be advertised whether or not they are advertisable. If the LLDP-MED capabilities TLV is not advertisable, the other LLDP-MED TLVs will not be advertised regardless of whether or not they are advertisable.

The port and protocol VLAN ID, VLAN name, and management VLAN ID TLVs in IEEE 802.1 organizationally specific LLDP TLVs can be configured only for nearest bridge agents. The configuration can be inherited by nearest customer bridge agents and nearest non-TPMR bridge agents.

Examples

Enable the nearest customer bridge agents on GigabitEthernet 1/0/1 to advertise link aggregation TLVs of the IEEE 802.1 organizationally specific TLVs.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp agent nearest-customer tlv-enable dot1-tlv
link-aggregation
```

lldp tlv-enable private-tlv

Use **lldp tlv-enable private-tlv** to specify types of H3C-proprietary TLVs advertisable on an interface.

Use **undo lldp tlv-enable private-tlv** to disable advertising H3C-proprietary TLVs on an interface.

NOTE:

- This command is supported only on PoE devices.
- This command is supported only in Release 6343P08 and later.

Syntax

lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **tlv-enable private-tlv actual-power**

undo lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **tlv-enable private-tlv actual-power**

Default

No H3C-proprietary TLVs can be advertised on an interface.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

agent: Specifies an agent type. If you do not specify an agent type, the command specifies types of H3C- proprietary TLVs that can be advertised by nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

actual-power: Specifies actual power TLVs.

Usage guidelines

H3C-proprietary TLVs are defined to meet specific transmission requirements on network management. Devices of other vendors cannot identify H3C-proprietary TLVs carried in LLDPDUs.

Only actual power TLVs are supported in the current software version. This type of TLV provides PoE power information on an interface.

Examples

Configure nearest customer bridge agents to advertise actual power TLVs on interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp agent neareset-customer tlv-enable private-tlv
actual-power
```

reset lldp statistics

Use **reset lldp statistics** to clear LLDP statistics on ports.

Syntax

reset lldp statistics [**interface** *interface-type interface number*] [**agent** { **nearest-bridge** | **nearest-customer** | **nearest-nontpmr** }]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify this option, the command clears LLDP statistics on all ports.

agent: Specifies an agent type. If you do not specify an agent type, the command clears LLDP statistics for all LLDP agents.

nearest-bridge: Specifies nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

nearest-nontpmr: Specifies nearest non-TPMR bridge agents.

Usage guidelines

If you do not specify any parameters, the **reset lldp statistics** command clears LLDP statistics on all ports but does not clear global LLDP statistics.

Examples

Clear LLDP statistics on all ports.

```
<Sysname> reset lldp statistics
```

Related commands

display lldp statistic

Contents

L2PT commands

display l2protocol statistics

Use **display l2protocol statistics** to display Layer 2 Protocol Tunneling (L2PT) statistics.

Syntax

display l2protocol statistics [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a Layer 2 Ethernet or aggregate interface by its type and number. If you do not specify this option, the command displays L2PT statistics for all Layer 2 Ethernet and aggregate interfaces.

Examples

Display L2PT statistics for all Layer 2 Ethernet and aggregate interfaces.

```
<Sysname> display l2protocol statistics
L2PT statistics information on interface Bridge-Aggregation1:
Protocol  Encapsulated      Decapsulated      Forwarded         Dropped
CDP       0                 0                 0                 0
DLDP      0                 3                 0                 0
EOAM      0                 2                 0                 0
GVRP      8                 4                 9                 2
LACP      0                 0                 0                 0
LLDP      0                 3                 0                 0
MVRP      0                 0                 0                 0
PAGP      0                 1                 0                 0
PVST      0                 0                 0                 0
STP       5                 5                 5                 0
Tunnel    N/A               N/A               100               10
VTP       0                 6                 0                 0
UDLD      0                 0                 0                 0
DTP       0                 0                 0                 0
CFD       0                 0                 0                 0

L2PT statistics information on interface GigabitEthernet1/0/1:
Protocol  Encapsulated      Decapsulated      Forwarded         Dropped
CDP       0                 0                 0                 0
DLDP      2                 3                 3                 0
EOAM      5                 2                 9                 0
GVRP      8                 4                 9                 2
```

```
LACP        0                 0                 0                 0
LLDP        3                 3                 3                 3
MVRP        0                 0                 0                 0
PAGP        5                 1                 7                 3
PVST        0                 0                 0                 0
STP         5                 5                 5                 0
Tunnel      N/A               N/A               100               10
VTP         0                 6                 0                 0
UDLD        0                 0                 0                 0
DTP         0                 0                 0                 0
CFD         0                 0                 0                 0
```

Table 1 Command output

Field	Description
Protocol	Protocol. The DTP and CFD protocols are supported only in Release 6331 and later.
Encapsulated	Number of encapsulated packets. The number increases by 1 when the interface receives and encapsulates a protocol packet from a customer network. For protocol **Tunnel**, which represents tunneled packets, this field displays **N/A**.
Decapsulated	Number of decapsulated packets. The number increases by 1 when the interface receives and decapsulates a tunneled packet from the service provider network. For protocol **Tunnel**, which represents tunneled packets, this field displays **N/A**.
Forwarded	Number of forwarded packets. The number increases by 1 when the interface receives a protocol packet and forwards it. The number increases by 1 for protocol **Tunnel** when the interface receives a tunneled packet and forwards it. If no interface of the PE is connected to customer networks, the number does not increase.
Dropped	Number of dropped packets. The number increases by 1 when the interface receives a protocol packet and drops it. Protocol packets dropped by hardware are not counted. The number increases by 1 for protocol **Tunnel** when the interface receives a tunneled packet and drops it.

l2protocol tunnel dot1q

Use **l2protocol tunnel dot1q** to enable L2PT for a protocol.

Use **undo l2protocol tunnel dot1q** to disable L2PT for a protocol.

Syntax

In Layer 2 Ethernet interface view:

l2protocol { **cdp** | **cfd** | **dldp** | **dtp** | **eoam** | **gvrp** | **lacp** | **lldp** | **mvrp** | **pagp** | **pvst** | **stp** | **udld** | **vtp** } **tunnel dot1q**

undo l2protocol { **cdp** | **cfd** | **dldp** | **dtp** | **eoam** | **gvrp** | **lacp** | **lldp** | **mvrp** | **pagp** | **pvst** | **stp** | **udld** | **vtp** } **tunnel dot1q**

In Layer 2 aggregate interface view:

l2protocol { **cdp** | **cfd** | **gvrp** | **lacp** | **lldp** | **mvrp** | **pagp** | **pvst** | **stp** | **udld** | **vtp** } **tunnel dot1q**

undo l2protocol { **cdp** | **cfd** | **gvrp** | **lacp** | **lldp** | **mvrp** | **pagp** | **pvst** | **stp** | **udld** | **vtp** } **tunnel dot1q**

Default

L2PT is disabled for all protocols.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

cdp: Specifies CDP.

cfd: Specifies CFD.

dldp: Specifies DLDP.

dtp: Specifies DTP.

eoam: Specifies EOAM.

gvrp: Specifies GVRP.

lacp: Specifies LACP.

lldp: Specifies LLDP. L2PT for LLDP supports LLDP packets from only nearest bridge agents.

mvrp: Specifies MVRP.

pagp: Specifies PAgP.

pvst: Specifies PVST.

stp: Specifies STP.

udld: Specifies UDLD.

vtp: Specifies VTP.

NOTE:

The **dtp** and **cfd** keywords are supported only in Release 6331 and later.

Usage guidelines

Before you enable L2PT for a protocol on a port, perform the following tasks:

- Enable the protocol on the CE, and disable the protocol on the port.
- Enable L2PT only on customer-facing PE ports. If you enable L2PT on ports connected to the service provider network, L2PT determines that the ports are connected to a customer network.
- Disable the protocol (for example, STP) on the PE ports connecting to an aggregate interface on a CE when the following conditions exist:
  - The protocol is running on the aggregate interface on the CE.
  - The aggregate interface on the CE connects to an L2PT-enabled port on the PE.

You can enable L2PT on member ports of a Layer 2 aggregation group, but the configuration does not take effect.

Examples

Disable STP and enable L2PT for STP on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo stp enable
[Sysname-GigabitEthernet1/0/1] l2protocol stp tunnel dot1q
```

Disable STP and enable L2PT for STP on Bridge-Aggregation 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] undo stp enable
[Sysname-Bridge-Aggregation1] l2protocol stp tunnel dot1q
```

l2protocol tunnel-dmac

Use **l2protocol tunnel-dmac** to set the destination multicast MAC address for tunneled packets of all protocols.

Use **undo l2protocol tunnel-dmac** to restore the default.

Syntax

l2protocol tunnel-dmac *mac-address*

undo l2protocol tunnel-dmac

Default

The tunneled packets use 010f-e200-0003 as the destination multicast MAC address.

Views

System view

Predefined user roles

network-admin

Parameters

mac-address: Specifies a destination multicast MAC address. The available addresses are 0100-0ccd-cdd0, 0100-0ccd-cdd1, 0100-0ccd-cdd2, and 010f-e200-0003.

Usage guidelines

The **l2protocol tunnel-dmac** command sets the destination multicast MAC address for tunneled packets of all protocols. The **l2protocol type tunnel-dmac** command sets the destination multicast MAC address for tunneled packets of the specified protocol. If both commands are executed, the **l2protocol type tunnel-dmac** command takes priority.

NOTE:

The **l2protocol type tunnel-dmac** command is supported only in Release 6331 and later.

Examples

Set the destination multicast MAC address to 0100-0ccd-cdd0 for tunneled packets.

```
<Sysname> system-view
[Sysname] l2protocol tunnel-dmac 0100-0ccd-cdd0
```

Related commands

l2protocol type tunnel-dmac

l2protocol type tunnel-dmac

Use **l2protocol type tunnel-dmac** to set the destination multicast MAC address for tunneled packets of the specified protocol.

Use **undo l2protocol type tunnel-dmac** to restore the default.

NOTE:

The **l2protocol type tunnel-dmac** command is supported only in Release 6331 and later.

Syntax

l2protocol type { **cdp** | **cfd** | **dldp** | **dtp** | **eoam** | **gvrp** | **lacp** | **lldp** | **mvrp** | **pagp** | **pvst** | **stp** | **udld** | **vtp** } **tunnel-dmac** *mac-address*

undo l2protocol type { **cdp** | **cfd** | **dldp** | **dtp** | **eoam** | **gvrp** | **lacp** | **lldp** | **mvrp** | **pagp** | **pvst** | **stp** | **udld** | **vtp** } **tunnel-dmac**

Default

The tunneled packets of all protocols use 010f-e200-0003 as the destination multicast MAC address.

Views

System view

Predefined user roles

network-admin

Parameters

cdp: Specifies CDP.

cfd: Specifies CFD.

dldp: Specifies DLDP.

dtp: Specifies DTP.

eoam: Specifies EOAM.

gvrp: Specifies GVRP.

lacp: Specifies LACP.

lldp: Specifies LLDP.

mvrp: Specifies MVRP.

pagp: Specifies PAgP.

pvst: Specifies PVST.

stp: Specifies STP.

udld: Specifies UDLD.

vtp: Specifies VTP.

mac-address: Specifies a destination multicast MAC address for tunneled packets of the specified protocol, in the range of 0100-0000-0000 to 01ff-ffff-ffff.

Usage guidelines

The **l2protocol tunnel-dmac** command sets the destination multicast MAC address for tunneled packets of all protocols. This command sets the destination multicast MAC address for

tunneled packets of the specified protocol. If both commands are executed, the **l2protocol type tunnel-dmac** command takes priority.

For tunneled packets to be recognized, set the same destination multicast MAC address for packets of the same protocol on PEs that are connected to the same customer network.

If you execute this command multiple times for a protocol, the most recent configuration takes effect.

Examples

Set the destination multicast MAC address to 0100-0ccd-cddc for tunneled packets of CFD.

```
<Sysname> system-view
[Sysname] l2protocol type cfd tunnel-dmac 0100-0ccd-cddc
```

Related commands

l2protocol tunnel-dmac

reset l2protocol statistics

Use **reset l2protocol statistics** to clear L2PT statistics.

Syntax

reset l2protocol statistics [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a Layer 2 Ethernet or aggregate interface by its type and number. If you do not specify this option, the command clears L2PT statistics on all Layer 2 Ethernet and aggregate interfaces.

Examples

Clear L2PT statistics on all Layer 2 Ethernet and aggregate interfaces.

```
<Sysname> reset l2protocol statistics
```

Contents

PPPoE relay commands

PPPoE relay commands

display pppoe-relay client-information

Use **display pppoe-relay client-information** to display the vendor-specific tag processing configuration for client-side packets on the PPPoE relay.

Syntax

display pppoe-relay client-information { **format** | **strategy** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

format: Displays the format configuration for the vendor-specific tag processing for client-side packets on the PPPoE relay.

strategy: Displays the policy configuration for the vendor-specific tag processing for client-side packets on the PPPoE relay.

Examples

Display the format configuration for the vendor-specific tag processing for client-side packets on the PPPoE relay.

```
<Sysname> display pppoe-relay client-information format
The current client-information format:
Circuit ID: ASCII
Remote ID: ASCII
```

Display the policy configuration for the vendor-specific tag processing for client-side packets on the PPPoE relay.

```
<Sysname> display pppoe-relay client-information strategy
The current global client-information strategy: Replace
The current interface client-information strategy:
  Interface                      Strategy
  GigabitEthernet1/0/1           Keep
  GigabitEthernet1/0/2           Drop
```

Table 1 Command output

Field	Description
The current client-information format	Circuit ID and remote ID padding formats in the vendor-specific tag: • **ASCII**—ASCII string padding format. • **Hex**—Hexadecimal padding format. • **User-defined**—User-defined padding format.
The current global	Global vendor-specific tag processing policy for the client-side PADI and

Field	Description
client-information strategy	PADR packets on the PPPoE relay: • **Drop**—Strips the vendor-specific tag from the PADI or PADR packets. • **Keep**—Keeps the vendor-specific tag unchanged. • **Replace**—Pads the vendor-specific tag in the configured padding format.
The current interface client-information strategy	Interface-level vendor-specific tag processing policy for the client-side PADI and PADR packets on the PPPoE relay.
Interface	Interface name. This field displays only the interfaces whose processing policies are different from the global processing policy.
Strategy	Vendor-specific tag processing policy for the client-side PADI and PADR packets of the interface on the PPPoE relay: • **Drop**—Strips the vendor-specific tag from the PADI or PADR packets. • **Keep**—Keeps the vendor-specific tag unchanged. • **Replace**—Pads the vendor-specific tag in the configured padding format.

Related commands

pppoe-relay client-information format

pppoe-relay client-information strategy

display pppoe-relay statistics

Use **display pppoe-relay statistics** to display packets statistics for the PPPoE relay.

Syntax

display pppoe-relay statistics [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

Usage guidelines

When this command is executed, this command displays statistics only for packets with non-zero packet counts.

Examples

Display packet statistics on GigabitEthernet 1/0/1.

```
<Sysname> display pppoe-relay statistics interface GigabitEthernet 1/0/1
Interface: GigabitEthernet1/0/1
  Packets received:
    ALL = 5 PADI = 5 PADO = 0 PADR = 0 PADS = 0 PADT = 0
  Packets sent:
```

```
    ALL = 5 PADI = 0 PADO = 5 PADR = 0 PADS = 0 PADT = 0
  Packets dropped:
    Server responses from untrusted ports = 0
    Client requests towards untrusted ports = 0
    Malformed PPPoE Discovery packets = 0
```

Table 2 Command output

Field	Description
Interface	Statistics on an interface.
Packets received	Incoming packet statistics of the interface: • **ALL**—Number of all PAD packets. • **PADI**—Number of PADI packets. • **PADO**—Number of PADO packets. • **PADR**—Number of PADR packets. • **PADS**—Number of PADS packets. • **PADT**—Number of PADT packets.
Packets sent	Outgoing packet statistics of the interface: • **ALL**—Number of all PAD packets. • **PADI**—Number of PADI packets. • **PADO**—Number of PADO packets. • **PADR**—Number of PADR packets. • **PADS**—Number of PADS packets. • **PADT**—Number of PADT packets.
Packets dropped	Dropped packets statistics of the interface.
Server responses from untrusted ports	Number of PADO and PADS packets dropped on untrusted ports.
Client requests towards untrusted ports	Number of PADR packets dropped by untrusted ports.

Related commands

reset pppoe-relay statistics

pppoe-relay client-information format

Use **pppoe-relay client-information format** to configure the circuit ID and remote ID padding formats for the client-side PPPoE packets on the PPPoE relay.

Use **undo pppoe-relay client-information format** to restore the default.

Syntax

pppoe-relay client-information format { **circuit-id** | **remote-id** } { **ascii** | **hex** | **user-defined** *text* }

undo pppoe-relay client-information format { **circuit-id** | **remote-id** }

Default

Both the circuit ID padding format and the remote ID padding format for the client-side PPPoE packets are the ASCII string on the PPPoE relay.

Views

System view

Predefined user roles

network-admin

Parameters

circuit-id: Specifies the circuit ID padding format.

remote-id: Specifies the remote ID padding format.

ascii: Specifies the ASCII string format. When this format is configured, **"**%portname:%svlan.%cvlan %sysname**"** is extracted and used as the circuit ID content, and **"**%mac**"** is used as the remote ID content. The circuit ID and remote ID are padded with the corresponding contents in the ASCII string format.

hex: Specifies the hexadecimal format. When this format is configured, **"**%length%port%svlan%cvlan**"** is extracted and used as the circuit ID content, and **"**%length%mac**"** is used as the remote ID content. The circuit ID and remote ID are padded with the corresponding contents in the hexadecimal format.

user-defined *text*: Specifies the user-defined format. The *text* argument is a case-sensitive string of 1 to 127 characters. When this format is configured, the corresponding information is extracted from the configured text and padded in the circuit ID and remote ID.

Usage guidelines

When the PPPoE relay receives PPPoE packets from the PPPoE client, the PPPoE relay pads the circuit ID and remote ID with the contents in the format configured by using this command.

Both the circuit ID and remote ID are of up to 63 characters. When the content to be padded exceeds 63 characters, the first 63 characters are padded.

When the user-defined format is used, the system automatically recognizes the escape keyword input by the user and translates it to the actual information. For more information about the supported escape keywords, see Table 3. For example, suppose the interface that receives packet on the PPPoE relay is GigabitEthernet 1/0/1. In this case, you can input the escape keyword **%portname**. Then, the system automatically recognizes the escape keyword and translates the escape keyword into the actual port information GigabitEthernet 1/0/1. For the system to correctly recognize the escape keywords, you must add the dollar sign (%) before each keyword. Otherwise, the system directly uses the input keyword and does not translate it. Non-escape keywords are directly used.

An integer can be added between the dollar sign (%) and the escape keyword. The integer specifies the width of the translated characters. When the translated characters do not reach the width specified by the integer, spaces are padded on the left to fill the width.

Table 3 Description of escape keywords supported by the user-defined format

Keyword	Description
sysname	System name of the PPPoE relay.
portname	Port name.
porttype	Port type.
slot	Slot number of the port.
subslot	Subslot number of the port.
port	Port number.
svlan	Outer VLAN ID.
cvlan	Inner VLAN ID.
mac	MAC address of the PPPoE relay.
Length	Length of the subsequent string. The padded content is of double digits.

Keyword	Description
	When the length is a single digit, one digit of 0 is padded on the left.

When you use different padding formats, the packet contents are different. For example, the contents of the circuit ID are as follows: the user access interface is GigabitEthernet 1/0/1, the outer VLAN ID is 200, the inner VLAN ID is 100, and the system name of the PPPoE relay is Sysname. The contents of the remote ID are as follows: the MAC address of the PPPoE relay is 04f9-38a9-44b0.

When you use the ASCII string format, the contents are as follows:

```
Circuit ID: GigabitEthernet1/0/1:200.100 Sysname
Remote ID: 04f9-38a9-44b0
```

When you use the hexadecimal format, the contents are as follows:

```
Circuit ID: 00 05 00 00 c8 00 64
Remote ID: 00 06 04 f9 38 a9 44 b0
```

When you use the user-defined format, the contents are as follows:

Configure the user-defined format "%portname:%svlan.%cvlan %sysname" for the circuit ID.

```
[Sysname] pppoe-relay client-information format circuit-id user-defined
"%portname:%svlan.%cvlan %sysname"
```

Configure the user-defined format %mac for the remote ID.

```
[Sysname] pppoe-relay client-information format remote-id user-defined "%mac"
```

Examples

Configure the circuit ID padding format as the ASCII string format for the client-side PPPoE packets on the PPPoE relay.

```
<Sysname> system-view
[Sysname] pppoe-relay client-information format circuit-id ascii
```

Related commands

display pppoe-relay client-information

pppoe-relay client-information strategy

pppoe-relay client-information strategy

Use **pppoe-relay client-information strategy** to configure the vendor-specific tag processing policy for the client-side PADI and PADR packets on the PPPoE relay.

Use **undo pppoe-relay client-information strategy** to restore the default.

Syntax

pppoe-relay client-information strategy { **drop** | **keep** | **replace** }

undo pppoe-relay client-information strategy

Default

The global vendor-specific tag processing policy for the client-side PADI and PADR packets on the PPPoE relay is replace.

No interface-level vendor-specific tag processing policy for the client-side PADI and PADR packets on the PPPoE relay is configured.

Views

System view

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

drop: Strips the vendor-specific tag from the PADI or PADR packets.

keep: Keeps the vendor-specific tag unchanged.

replace: Pads the vendor-specific tag in the configured format.

Usage guidelines

This feature can be configured both in system view and in interface view. The configuration in system view takes effect on all interfaces. The configuration in interface view takes effect only on the current interface. The configuration in interface view takes precedence over the configuration in system view.

The processing policy takes effect only on incoming packets of interfaces.

This command is not supported on Layer 2 aggregation group member ports. If a Layer 2 Ethernet interface is configured with this command before joining a Layer 2 aggregation group, the command is cleared on the member port after the member ports joins the aggregation group.

Examples

Configure the global processing policy for the client-side PADI and PADR packets as drop on the PPPoE relay.

```
<Sysname> system-view
[Sysname] pppoe-relay client-information strategy drop
```

Related commands

display pppoe-relay client-information

pppoe-relay client-information format

pppoe-relay enable

Use **pppoe-relay enable** to enable the PPPoE relay function.

Use **undo pppoe-relay enable** to disable the PPPoE relay function.

Syntax

pppoe-relay enable

undo pppoe-relay enable

Default

The PPPoE relay function is disabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable the PPPoE relay function.

```
<Sysname> system-view
```

```
[Sysname] pppoe-relay enable
```

pppoe-relay server-information vendor-specific strip

Use **pppoe-relay server-information vendor-specific strip** to enable an interface to strip the vendor-specific tags of the PPPoE server-side packets.

Use **undo pppoe-relay server-information vendor-specific strip** to disable an interface from stripping the vendor-specific tags of the PPPoE server-side packets.

Syntax

pppoe-relay server-information vendor-specific strip

undo pppoe-relay server-information vendor-specific strip

Default

The function of stripping vendor-specific tags of the PPPoE server-side packets is disabled on an interface.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

When the PPPoE relay receives PADO and PADS packets from the PPPoE server on a PPPoE relay trusted port with this feature enabled, the PPPoE relay strips the vendor-specific tags of the packets before forwarding the packets.

This command takes effect only on packets received on PPPoE relay trusted ports.

This command is not supported on Layer 2 aggregation group member ports. If a Layer 2 Ethernet interface is configured with this command before joining a Layer 2 aggregation group, the command is cleared on the member port after the member ports joins the aggregation group.

Examples

Enable GigabitEthernet 1/0/1 to strip the vendor-specific tags of the PPPoE server-side packets..

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] pppoe-relay trust
[Sysname-GigabitEthernet1/0/1] pppoe-relay server-information vendor-specific strip
```

Related commands

pppoe-relay trust

pppoe-relay trust

Use **pppoe-relay trust** to configure an interface as PPPoE relay trusted port.

Use **undo pppoe-relay trust** to restore the default.

Syntax

pppoe-relay trust

undo pppoe-relay trust

Default

An interface is a PPPoE relay untrusted port.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

A PPPoE relay-enabled device processes PPPoE protocol packets as follows:

- When receiving PADI, PADR, and PADT on untrusted ports, the device can forward the packets out of only the trusted ports.
- When receiving PADO and PADS packets on untrusted ports, the device directly drops the packets.
- When receiving PADO, PADS, and PADT packets on trusted ports, the device can forward the packets out of any port.
- When receiving PADI and PADR packets on trusted ports, the device can forward the packets out of only the trusted ports.

For a PPPoE relay to correctly forward and process PPPoE protocol packets, you must configure the PPPoE server-facing interfaces on the PPPoE relay as trusted ports, and configure the PPPoE client-facing interfaces on the PPPoE relay as untrusted ports.

This command is not supported on Layer 2 aggregation group member ports. If a Layer 2 Ethernet interface is configured with this command before joining a Layer 2 aggregation group, the command is cleared on the member port after the member ports joins the aggregation group.

Examples

Configure GigabitEthernet 1/0/1 as a PPPoE relay trusted port.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] pppoe-relay trust
```

Related commands

pppoe-relay server-information vendor-specific strip

reset pppoe-relay statistics

Use **reset pppoe-relay statistics** to clear packets statistics for the PPPoE relay.

Syntax

reset pppoe-relay statistics

Views

User view

Predefined user roles

network-admin

Examples

Clear packet statistics for the PPPoE relay.

```
<Sysname> reset pppoe-relay statistics
```

Related commands

`reset pppoe-relay statistics`

Layer 3—IP Services Command Reference

This command reference is applicable to the following switches and software versions:

H3C S5120V2-LI switch series (Release 6308P01 and later)
H3C S3100V3-SI switch series (Release 6309P01 and later)
H3C S5110V2 switch series (Release 6310 and later)
H3C S5110V2-SI switch series (Release 6310 and later)
H3C S5000V3-EI switch series (Release 6310 and later)
H3C S5000V5-EI switch series (Release 6319P01 and later)
H3C S5000E-X switch series (Release 6310 and later)
H3C S5130S-LI switch series (Release 6310 and later)
H3C MS4320V2 switch series (Release 6308P01 and later)
H3C MS4320 switch series (Release 6308P01 and later)
H3C MS4300V2 switch series (Release 6308P01 and later)
H3C MS4200 switch series (Release 6310 and later)
H3C WS5810-WiNet switch series (Release 6308P01 and later)
H3C WS5820-WiNet switch series (Release 6308P01 and later)
H3C WAS6000 switch series (Release 6308P01 and later)
H3C S5000X-EI switch series (Release 6329 and later)
H3C MS4320V3 switch series (Release 6329 and later)
H3C S5120V3-SI switch series (Release 6329 and later)
H3C S5120V3-LI switch series (Release 6329 and later)

New H3C Technologies Co., Ltd.
http://www.h3c.com

Software version: Release 63xx
Document version: 6W105-20230524

Preface

This command reference describes IP services configuration commands.

This preface includes the following topics about the documentation:

- Audience
- Conventions
- Documentation feedback

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Documentation feedback

You can e-mail your comments about product documentation to info@h3c.com.

We appreciate your comments.

Contents

ARP commands

arp check enable

Use **arp check enable** to enable dynamic ARP entry check.

Use **undo arp check enable** to disable dynamic ARP entry check.

Syntax

arp check enable

undo arp check enable

Default

Dynamic ARP entry check is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Dynamic ARP entry check disables a device from supporting dynamic ARP entries with multicast MAC addresses. The device cannot learn dynamic ARP entries containing multicast MAC addresses. You cannot manually add static ARP entries that contain multicast MAC addresses.

When dynamic ARP entry check is disabled, ARP entries containing multicast MAC addresses are supported. The device can learn dynamic ARP entries containing multicast MAC addresses obtained from the ARP packets sourced from a unicast MAC address. You can also manually add static ARP entries containing multicast MAC addresses.

Examples

Enable dynamic ARP entry check.

```
<Sysname> system-view
[Sysname] arp check enable
```

arp check log enable

Use **arp check log enable** to enable the ARP logging feature.

Use **undo arp check log enable** to disable the ARP logging feature.

Syntax

arp check log enable

undo arp check log enable

Default

ARP logging is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This feature enables a device to log ARP events when ARP cannot resolve IP addresses correctly. The log information helps administrators locate and solve problems. The device can log the following ARP events:

- On a proxy ARP-disabled interface, the target IP address of a received ARP packet is not one of the following IP addresses:
  - The IP address of the receiving interface.
  - The virtual IP address of the VRRP group.
- The sender IP address of a received ARP reply conflicts with one of the following IP addresses:
  - The IP address of the receiving interface.
  - The virtual IP address of the VRRP group.

The device sends ARP log messages to the information center. You can use the **info-center source** command to specify the log output rules for the information center. For more information about information center, see *Network Management and Monitoring Configuration Guide*.

The device can generate a large number of ARP logs. To conserve system resources, enable ARP logging only when you are auditing or troubleshooting ARP events.

Examples

Enable ARP logging.

```
<Sysname> system-view
[Sysname] arp check log enable
```

arp mac-interface-consistency check enable

Use **arp mac-interface-consistency check enable** to enable interface consistency check between ARP and MAC address entries.

Use **undo arp mac-interface-consistency check enable** to disable this feature.

Syntax

arp mac-interface-consistency check enable

undo arp mac-interface-consistency check enable

Default

Interface consistency check between ARP and MAC address entries is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

In an unstable network, the receiving interface for packets from a user might change. The interface in the MAC address entry can be updated immediately while the interface in the ARP entry cannot. In this case, the packets matching the ARP entry will be sent out of an incorrect interface. To solve this problem, you can use this feature to periodically check the interface consistency between the ARP and MAC address entry for a user. If the interfaces are not the same, ARP sends ARP requests in the VLAN of the ARP entry and updates the entry with the ARP reply receiving interface.

Use **display mac-address** to display MAC address entries.

Examples

Enable interface consistency check between ARP and MAC address entries.

```
<Sysname> system-view
[Sysname] arp mac-interface-consistency check enable
```

Related commands

display mac-address (*Layer 2—LAN Switching Command Reference*)

arp max-learning-num

Use **arp max-learning-num** to set the dynamic ARP learning limit for an interface.

Use **undo arp max-learning-num** to restore the default.

Syntax

arp max-learning-num *max-number* [**alarm** *alarm-threshold*]

undo arp max-learning-num

Default

The following matrix shows the default values for the dynamic ARP learning limit:

Hardware	Dynamic ARP learning limit on an interface
S5110V2-SI switch series S5000V3-EI switch series S5000V5-EI switch series S5000E-X switch series S5000X-EI switch series	128
WAS6000 switch series	• WAS6124-X and WAS6108: 1024 • Other switches: 128
S5110V2 switch series	256
WS5810-WiNet switch series	512
S5120V2-LI switch series S5130S-LI switch series S5120V3-SI switch series MS4320V2 switch series MS4320 switch series	1024
S3100V3-SI switch series	• Switches with product codes LS-3100V3-28TP-SI-H1, LS-3100V3-18TP-SI-H1, LS-3100V3-52TP-SI-H1, and LS-3100V3-20TP-PWR-SI-H1: 512 • Other switches: 1024
MS4200 switch series	• Switches with product codes LS-MS4200-28TP-H1, LS-MS4200-20TP-PWR-H1, and LS-MS4200-18TP-H1: 512 • Other switches: 1024
WS5820-WiNet switch series	• WS5820-28P-POE-WiNet: 512 • Other switches: 1024

Hardware	Dynamic ARP learning limit on an interface
MS4300V2 switch series	• MS4300V2-28P, MS4300V2-52P: 512 • Other switches: 1024
MS4320V3 switch series	• MS4320V3-28P, MS4320V3-52P: 512 • Other switches: 1024
S5120V3-LI switch series	• S5120V3-20P-LI, S5120V3-28P-LI, S5120V3-52P-LI, S5120V3-28P-PWR-LI, S5120V3-52P-PWR-LI: 512 • Other switches: 1024

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

VLAN interface view

Predefined user roles

network-admin

Parameters

max-number: Specifies the maximum number of dynamic ARP entries for an interface. The following matrix shows the value range for this argument:

Hardware	Value range
S5110V2-SI switch series S5000V3-EI switch series S5000V5-EI switch series S5000E-X switch series S5000X-EI switch series	0 to 128
WAS6000 switch series	• WAS6124-X and WAS6108: 0 to 1024 • Other switches: 0 to 128
S5110V2 switch series	0 to 256
WS5810-WiNet switch series	0 to 512
S5120V2-LI switch series S5130S-LI switch series S5120V3-SI switch series MS4320V2 switch series MS4320 switch series	0 to 1024
S3100V3-SI switch series	• Switches with product codes LS-3100V3-28TP-SI-H1, LS-3100V3-18TP-SI-H1, LS-3100V3-52TP-SI-H1, and LS-3100V3-20TP-PWR-SI-H1: 0 to 512 • Other switches: 0 to 1024
MS4200 switch series	• Switches with product codes LS-MS4200-28TP-H1, LS-MS4200-20TP-PWR-H1, and LS-MS4200-18TP-H1: 0 to 512 • Other switches: 0 to 1024
WS5820-WiNet switch series	• WS5820-28P-POE-WiNet: 0 to 512

Hardware	Value range
	• Other switches: 0 to 1024
MS4300V2 switch series	• MS4300V2-28P, MS4300V2-52P: 0 to 512 • Other switches: 0 to 1024
MS4320V3 switch series	• MS4320V3-28P, MS4320V3-52P: 0 to 512 • Other switches: 0 to 1024
S5120V3-LI switch series	• S5120V3-20P-LI, S5120V3-28P-LI, S5120V3-52P-LI, S5120V3-28P-PWR-LI, S5120V3-52P-PWR-LI: 0 to 512 • Other switches: 0 to 1024

alarm *alarm-threshold*: Specifies an alarm threshold for dynamic ARP learning, in percentage. The value range for the *alarm-threshold* argument is 1 to 100. The device generates a log message when the number of dynamic ARP entries learned on an interface reaches the value calculated by using the formula: (*max-number* × *alarm-threshold*)/100. If you do not specify the alarm threshold, the device does not generate log messages.

Usage guidelines

An interface can dynamically learn ARP entries. To prevent an interface from holding too many ARP entries, you can set the maximum number of dynamic ARP entries that the interface can learn. When the maximum number is reached, the interface stops learning ARP entries.

When the *number* argument is set to 0, the interface is disabled from learning dynamic ARP entries.

Examples

Specify VLAN-interface 40 to learn a maximum of 10 dynamic ARP entries.

```
<Sysname> system-view
[Sysname] interface vlan-interface 40
[Sysname-Vlan-interface40] arp max-learning-num 10
```

Specify GigabitEthernet 1/0/1 to learn a maximum of 10 dynamic ARP entries.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp max-learning-num 10
```

Specify Layer 2 aggregate interface Bridge-Aggregation 1 to learn a maximum of 10 dynamic ARP entries.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] arp max-learning-num 10
```

arp max-learning-number

Use **arp max-learning-number** to set the dynamic ARP learning limit for a device.

Use **undo arp max-learning-number** to restore the default.

Syntax

arp max-learning-number *max-number* **slot** *slot-number*

undo arp max-learning-number slot *slot-number*

Default

The following matrix shows the default values for the dynamic ARP learning limit:

Hardware	ARP learning limit on the device
S5110V2-SI switch series S5000V3-EI switch series S5000V5-EI switch series S5000E-X switch series S5000X-EI switch series	128
WAS6000 switch series	• WAS6124-X and WAS6108: 1024 • Other switches: 128
S5110V2 switch series	256
WS5810-WiNet switch series	512
S5120V2-LI switch series S5130S-LI switch series S5120V3-SI switch series MS4320V2 switch series MS4320 switch series	1024
S3100V3-SI switch series	• Switches with product codes LS-3100V3-28TP-SI-H1, LS-3100V3-18TP-SI-H1, LS-3100V3-52TP-SI-H1, and LS-3100V3-20TP-PWR-SI-H1: 512 • Other switches: 1024
MS4200 switch series	• Switches with product codes LS-MS4200-28TP-H1 LS-MS4200-20TP-PWR-H1, and LS-MS4200-18TP-H1: 512 • Other switches: 1024
WS5820-WiNet switch series	• WS5820-28P-POE-WiNet: 512 • Other switches: 1024
MS4300V2 switch series	• MS4300V2-28P, MS4300V2-52P: 512 • Other switches: 1024
MS4320V3 switch series	• MS4320V3-28P, MS4320V3-52P: 512 • Other switches: 1024
S5120V3-LI switch series	• S5120V3-20P-LI, S5120V3-28P-LI, S5120V3-52P-LI, S5120V3-28P-PWR-LI, S5120V3-52P-PWR-LI: 512 • Other switches: 1024

Views

System view

Predefined user roles

network-admin

Parameters

max-number: Specifies the maximum number of dynamic ARP entries for a device. The following matrix shows the value range for this argument:

Hardware	Value range
S5110V2-SI switch series	0 to 128

Hardware	Value range
S5000V3-EI switch series S5000V5-EI switch series S5000E-X switch series S5000X-EI switch series	
WAS6000 switch series	• WAS6124-X and WAS6108: 0 to 1024 • Other switches: 0 to 128
S5110V2 switch series	0 to 256
WS5810-WiNet switch series	0 to 512
S5120V2-LI switch series S5130S-LI switch series S5120V3-SI switch series MS4320V2 switch series MS4320 switch series	0 to 1024
S3100V3-SI switch series	• Switches with product codes LS-3100V3-28TP-SI-H1, LS-3100V3-18TP-SI-H1, LS-3100V3-52TP-SI-H1, and LS-3100V3-20TP-PWR-SI-H1: 0 to 512 • Other switches: 0 to 1024
MS4200 switch series	• Switches with product codes LS-MS4200-28TP-H1, LS-MS4200-20TP-PWR-H1, and LS-MS4200-18TP-H1: 0 to 512 • Other switches: 0 to 1024
WS5820-WiNet switch series	• WS5820-28P-POE-WiNet: 0 to 512 • Other switches: 0 to 1024
MS4300V2 switch series	• MS4300V2-28P, MS4300V2-52P: 0 to 512 • Other switches: 0 to 1024
MS4320V3 switch series	• MS4320V3-28P, MS4320V3-52P: 0 to 512 • Other switches: 0 to 1024
S5120V3-LI switch series	• S5120V3-20P-LI, S5120V3-28P-LI, S5120V3-52P-LI, S5120V3-28P-PWR-LI, S5120V3-52P-PWR-LI: 0 to 512 • Other switches: 0 to 1024

slot *slot-number*: Specifies an IRF member device by its member ID.

Usage guidelines

A device can dynamically learn ARP entries. To prevent a device from holding too many ARP entries, you can set the maximum number of dynamic ARP entries that the device can learn. When the maximum number is reached, the device stops learning ARP entries.

When the *number* argument is set to 0, the device is disabled from learning dynamic ARP entries.

Examples

Set the ARP learning limit to 64 for slot 1.

```
<Sysname> system-view
[Sysname] arp max-learning-number 64 slot 1
```

arp multiport

Use **arp multiport** to configure a multiport ARP entry.

Use **undo arp** to delete an ARP entry.

Syntax

arp multiport *ip-address mac-address vlan-id*

undo arp *ip-address*

Default

No multiport ARP entries exist.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies an IP address for the multiport ARP entry.

mac-address: Specifies a MAC address for the multiport ARP entry, in the format of H-H-H.

vlan-id: Specifies a VLAN for the multiport ARP entry, in the range of 1 to 4094. The specified VLAN must already exist.

Usage guidelines

If the corresponding VLAN or the VLAN interface is deleted, the multiport ARP entry is also deleted.

To make the multiport ARP entry effective for packet forwarding, you must configure a multicast or multiport unicast MAC address entry to specify multiple output interfaces. The MAC address entry must have the same MAC address and VLAN ID as the multiport ARP entry. In addition, the IP address in the multiport ARP entry must reside on the same subnet as the VLAN interface of the specified VLAN.

If an aggregate interface is the output interface of an entry and its member ports reside on multiple IRF member devices, the device cannot use the entry to forward packets. To resolve this issue, set the global link-aggregation load sharing mode to a mode other than source or destination MAC address-based by using the **link-aggregation global load-sharing mode** command. For more information about this command, see Ethernet link aggregation in *Layer 2—LAN Switching Command Reference*.

Examples

Configure a multiport ARP entry that contains IP address 202.38.10.2 and MAC address 00e0-fc01-0000 in VLAN 10.

```
<Sysname> system-view
[Sysname] arp multiport 202.38.10.2 00e0-fc01-0000 10
```

Related commands

display arp multiport

reset arp multiport

arp smooth

Use **arp smooth** to synchronize ARP entries from the master device to all subordinate devices.

Syntax

arp smooth

Views

User view

Predefined user roles

network-admin

Examples

Synchronize ARP entries from the master device to all subordinate devices.

```
<Sysname> arp smooth
```

arp static

Use **arp static** to configure a static ARP entry.

Use **undo arp** to delete an ARP entry.

Syntax

arp static *ip-address mac-address* [*vlan-id interface-type interface-number*]

undo arp *ip-address*

Default

No static ARP entries exist.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies an IP address for the static ARP entry.

mac-address: Specifies a MAC address for the static ARP entry, in the format of H-H-H.

vlan-id: Specifies the ID of a VLAN to which the static ARP entry belongs. The value range is 1 to 4094.

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

A static ARP entry is manually configured and maintained. It does not age out and cannot be overwritten by any dynamic ARP entry.

Static ARP entries can be short or long.

A resolved short static ARP entry becomes unresolved upon certain events, for example, when the resolved output interface goes down, or the corresponding VLAN or VLAN interface is deleted.

Long static ARP entries are effective or ineffective. Ineffective long static ARP entries cannot be used for packet forwarding. A long static ARP entry is ineffective when any of the following conditions exists:

- The IP address in the entry conflicts with a local IP address.
- No local interface has an IP address in the same subnet as the IP address in the ARP entry.

If you specify the *vlan-id interface-type interface-number* argument, follow these restrictions and guidelines:

- The interface can be an Ethernet interface or an aggregate interface.
- The VLAN and VLAN interface must already exist. The specified Ethernet interface must belong to the specified VLAN.
- The IP address of the VLAN interface and the IP address specified by the *ip-address* argument must be on the same network.
- A long static ARP entry for a VLAN is deleted if the VLAN or VLAN interface is deleted.

Examples

Configure a long static ARP entry that contains IP address 202.38.10.2, MAC address 00e0-fc01-0000, and output interface GigabitEthernet 1/0/1 in VLAN 10.

```
<Sysname> system-view
[Sysname] arp static 202.38.10.2 00e0-fc01-0000 10 gigabitethernet 1/0/1
```

Related commands

display arp

reset arp

arp timer aging

Use **arp timer aging** to set the aging timer for dynamic ARP entries.

Use **undo arp timer aging** to restore the default.

Syntax

arp timer aging { *aging-minutes* | **second** *aging-seconds* }

undo arp timer aging

Default

In system view, the aging timer for dynamic ARP entries is 20 minutes.

In interface view, the aging timer for dynamic ARP entries is the aging timer set in system view.

Views

System view

VLAN interface view

Predefined user roles

network-admin

Parameters

aging-minutes: Specifies the aging timer in minutes. The value range for this argument is 1 to 1440.

second *aging-seconds*: Specifies the aging timer in seconds. The value range for the *aging-seconds* argument is 5 to 86400.

Usage guidelines

Each dynamic ARP entry in the ARP table has a limited lifetime, called an aging timer. The aging timer of a dynamic ARP entry is reset each time the dynamic ARP entry is updated. Dynamic ARP entries that are not updated before their aging timers expire are deleted from the ARP table.

You can set the aging timer for dynamic ARP entries in system view or in interface view. The aging timer set in interface view takes precedence over the aging timer set in system view.

Set the aging timer for dynamic ARP entries as needed. For example, when you configure proxy ARP, set a short aging time so that invalid dynamic ARP entries can be deleted in a timely manner.

Examples

Set the aging timer for dynamic ARP entries to 10 minutes.

```
<Sysname> system-view
[Sysname] arp timer aging 10
```

Set the aging timer for dynamic ARP entries to 200 seconds.

```
<Sysname> system-view
[Sysname] arp timer aging second 200
```

Set the aging timer for dynamic ARP entries to 200 seconds on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] arp timer aging second 200
```

Related commands

arp timer aging probe-count

arp timer aging probe-interval

display arp timer aging

arp timer aging probe-count

Use **arp timer aging probe-count** to set the maximum number of probes for dynamic ARP entries.

Use **undo arp timer aging probe-count** to restore the default.

Syntax

arp timer aging probe-count *count*

undo arp timer aging probe-count

Default

In system view, the maximum number of probes is three for dynamic ARP entries.

In interface view, the maximum number of probes for dynamic ARP entries is the maximum probe count set in system view.

Views

System view

VLAN interface view

Predefined user roles

network-admin

Parameters

count: Specifies the maximum number of probes. The value range for this argument is 0 to 10. To disable the device from probing dynamic ARP entries, set the value to 0.

Usage guidelines

This probe mechanism keeps legal dynamic ARP entries valid and avoids unnecessary ARP resolution during later traffic forwarding. This probe feature sends ARP requests for the IP address in a dynamic ARP entry.

- If the device receives an ARP reply before the entry aging timer expires, the device resets the aging timer.
- If the device does not receive any ARP reply after the maximum number of probes is made, the device deletes the entry when the entry aging timer expires.

You can set the maximum number of probes in system view and in interface view. The probe count set in interface view takes precedence over the probe count set in system view.

Examples

Allow the device to perform a maximum of five probes for dynamic ARP entries.

```
<Sysname> system-view
[Sysname] arp timer aging probe-count 5
```

Allow the device to perform a maximum of five probes for dynamic ARP entries on VLAN-interface 2.

<Sysname> system-view

```
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] arp timer aging probe-count 5
```

Related commands

arp timer aging

arp timer aging probe-interval

arp timer aging probe-interval

Use **arp timer aging probe-interval** to set the interval for probing dynamic ARP entries.

Use **undo arp timer aging probe-interval** to restore the default.

Syntax

arp timer aging probe-interval *interval*

undo arp timer aging probe-interval

Default

In system view, the probe interval is 5 seconds.

In interface view, the probe interval equals the setting in system view.

Views

System view

VLAN interface view

Predefined user roles

network-admin

Parameters

Interval: Specifies the probe interval in seconds. The value rang is 1 to 60.

Usage guidelines

The probing feature keeps legal dynamic ARP entries valid and avoids unnecessary ARP resolution during later traffic forwarding.

Before a dynamic ARP entry is aged out, the device sends ARP requests for the IP address in the ARP entry.

- If the device receives an ARP reply during the probe interval, the device resets the aging timer.

- If the device does not receive any ARP reply during the probe interval, the device starts a new probe.
- If the maximum number probes are made, and still no ARP reply is received, the device deletes the entry.

You can set the probe interval in system view and in interface view. The probe interval in interface view takes precedence over the probe interval in system view.

Examples

Set the probe interval to 10 seconds for dynamic ARP entries.

```
<Sysname> system-view
[Sysname] arp timer aging probe-interval 10
```

Set the probe interval to 10 seconds for dynamic ARP entries on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] arp timer aging probe-interval 10
```

Related commands

arp timer aging

arp timer aging probe-count

arp user-ip-conflict record enable

Use **arp user-ip-conflict record enable** to enable recording user IP address conflicts.

Use **undo arp user-ip-conflict record enable** to disable recording user IP address conflicts.

Syntax

```
arp user-ip-conflict record enable
undo arp user-ip-conflict record enable
```

Default

The default differs depending on the software version, as shown below:

Versions	Default setting
Versions earlier than Release 6350	Recording user IP address conflicts is disabled.
Release 6350 and later	• If the device starts up with the initial configuration, recording user IP address conflicts is disabled. • If the device starts up with the factory defaults, recording user IP address conflicts is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This feature enables the device to detect and record user IP address conflicts. The device determines that a conflict occurs if an incoming non-gratuitous ARP packet has the same sender IP address as an existing ARP entry but a different sender MAC address. The device generates a user IP address conflict record, logs the conflict, and sends the log to the information center. For

information about the log destination and output rule configuration, see the information center in *Network Management and Monitoring Configuration Guide*.

An IRF member device can generate a maximum of 10 user IP address conflict logs per second.

To display user IP address conflict records, use the **display arp user-ip-conflict record** command.

Examples

Enable recording user IP address conflicts.

```
<Sysname> system-view
[Sysname] arp user-ip-conflict record enable
```

Related commands

display arp user-ip-conflict record

arp user-move record enable

Use **user-move record enable** to enable recording user port migrations.

Use **undo arp user-move record enable** to disable recording user port migrations.

Syntax

arp user-move record enable

undo arp user-move record enable

Default

Recording user port migrations is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Each IRF member device can generate a maximum of 10 user port migration logs per second.

To display user port migration records, use the **display arp user-move record** command.

Examples

Enable recording user port migration.

```
<Sysname> system-view
[Sysname] arp user-move record enable
```

Related commands

display arp user-move record

display arp

Use **display arp** to display ARP entries.

Syntax

display arp [[**all** | **dynamic** | **multiport** | **static**] [**slot** *slot-number*] | **vlan** *vlan-id* | **interface** *interface-type interface-number*] [**count** | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

`all`: Displays all ARP entries.

`dynamic`: Displays dynamic ARP entries.

`multiport`: Displays multiport ARP entries.

`static`: Displays static ARP entries.

`slot` *`slot-number`*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays ARP entries for the master device.

`vlan` *`vlan-id`*: Specifies a VLAN by its VLAN ID. The VLAN ID is in the range of 1 to 4094.

`interface` *`interface-type interface-number`*: Specifies an interface by its type and number. If you do not specify an interface, this command displays ARP entries for all interfaces.

`count`: Displays the number of ARP entries.

`verbose`: Displays detailed information about ARP entries.

Usage guidelines

This command displays information about ARP entries, including the IP address, MAC address, VLAN ID, output interface, entry type, and aging timer.

Examples

Display all ARP entries.

```
<Sysname> display arp all
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport  I-Invalid
IP address      MAC address    VLAN/VSI   Interface               Aging Type
1.1.1.1          02e0-f102-0023 1         GE1/0/1                 --    S
1.1.1.2          00e0-fc00-0001 12        GE1/0/2                 960   D
1.1.1.4          00e0-fe60-5000 0         --                      --    M
```

Display detailed information about all ARP entries.

```
IP address          : 1.1.1.1            MAC address    : 02e0-f102-0023
Type                : Static             Aging          : --
Interface           : GE1/0/1            VLAN           : 1
VPN instance        : --
Link ID             : --
Service instance    : 1
VXLAN ID            : --
VSI name            : --
VSI interface       : --
Nickname            : --

IP address          : 1.1.1.2            MAC address    : 0015-e944-adc5
Type                : Dynamic            Aging          : 960 sec
Interface           : GE1/0/2            VLAN           : 12
```

```
VPN instance        : --
Link ID             : --
Service instance    : --
VXLAN ID            : --
VSI name            : --
VSI interface       : --
Nickname            : --

IP address          : 1.1.1.4                 MAC address    : 00e0-fe60-5000
Type                : Multiport               Aging          : --
Interface           : --                      VLAN           : --
VPN instance        : --
Link ID             : --
Service instance    : --
VXLAN ID            : --
VSI name            : --
VSI interface       : --
Nickname            : --
```

Display the number of all ARP entries.

```
<Sysname> display arp all count
 Total number of entries : 3
```

Table 1 Command output

Field	Description
IP address	IP address in an ARP entry.
MAC address	MAC address in an ARP entry.
VLAN/VSI	ID of the VLAN to which the ARP entry belongs. This field displays hyphens (**--**) in either of the following situations: • The ARP entry is an unresolved short static ARP entry. • The output interface of the ARP entry does not belong to the VLAN.
Interface	Output interface in an ARP entry. This field displays hyphens (**--**) in either of the following situations: • The ARP entry is an unresolved short static ARP entry. • The ARP entry is a multiport ARP entry and has no output interface information. To obtain the output interface information of the multiport ARP entry, look up the MAC address table according to the MAC address in the ARP entry.
Link ID	This field is not supported in the current software version. Link ID in an ARP entry. This field displays hyphens (**--**) if the ARP entry does not belong to any VSI.
Aging	Aging time for an ARP entry in seconds. For a static ARP entry, this field always displays hyphens (**--**). The static ARP entry never ages out unless you delete it manually. For a dynamic ARP entry, this field displays hyphens (**--**) if the aging time is unknown.
Type	ARP entry type: • **D**—Dynamic. • **S**—Static.

Field	Description
	• **O**—OpenFlow. • **R**—Rule. • **M**—Multiport. • **I**—Invalid.
VPN instance	This field is not supported in the current software version. Name of VPN instance. If no VPN instance is configured for the ARP entry, this field displays hyphens (--).
Service instance	This field is not supported in the current software version. Ethernet service instance in an ARP entry. This field displays hyphens (**--**) if no Ethernet service instance is specified for the Layer 2 Ethernet interface or Layer 2 aggregate interface in the ARP entry.
VXLAN ID	This field is not supported in the current software version. ID of the VXLAN to which the ARP entry belongs. VXLAN ID is also called VNI. If the ARP entry does not belong to any VXLAN, this field displays hyphens (**--**).
VSI name	This field is not supported in the current software version. Name of the VSI to which the ARP entry belongs. If the ARP entry does not belong to any VSI, this field displays hyphens (**--**).
VSI interface	This field is not supported in the current software version. Name of the gateway interface of the VSI. If no gateway interface is specified for the VSI, this field displays hyphens (**--**).
Nickname	This field is not supported in the current software version. Nickname of the ARP entry. The nickname is a string of four hexadecimal numbers, for example, 012a.
Total number of entries	Number of ARP entries.

Related commands

`arp static`

`reset arp`

display arp entry-limit

Use **`display arp entry-limit`** to display the maximum number of ARP entries that a device supports.

Syntax

`display arp entry-limit`

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the maximum number of ARP entries that the device supports.

```
<Sysname> display arp entry-limit
```

```
ARP entries: 1024
```

display arp *ip-address*

Use **display arp** *ip-address* to display the ARP entry for an IP address.

Syntax

display arp *ip-address* [**slot** *slot-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ip-address: Displays the ARP entry for the specified IP address.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for the master device.

verbose: Displays the detailed information about the specified ARP entry.

Usage guidelines

The ARP entry information includes the IP address, MAC address, VLAN ID, output interface, entry type, and aging timer.

Examples

Display the ARP entry for the IP address 20.1.1.1.

```
<Sysname> display arp 20.1.1.1
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport  I-Invalid
IP address      MAC address    VLAN/VSI   Interface                Aging Type
20.1.1.1        00e0-fc00-0001 --         --                       --    S
```

Related commands

arp static

reset arp

display arp openflow count

Use **display arp openflow count** to display the number of OpenFlow ARP entries.

Syntax

display arp openflow count [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the number of OpenFlow ARP entries for the master device.

Examples

Display the number of OpenFlow ARP entries.

```
<Sysname> display arp openflow count
 Total number of OpenFlow ARP entries: 6
```

display arp timer aging

Use **display arp timer aging** to display the aging timer of dynamic ARP entries.

Syntax

display arp timer aging

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

This command always displays the aging time in seconds no matter which unit you set in the **arp timer aging** command.

Examples

Display the aging timer of dynamic ARP entries.

```
<Sysname> display arp timer aging
Current ARP aging time is 1200 seconds
```

Related commands

arp timer aging

display arp user-ip-conflict record

Use **display arp user-ip-conflict record** to display user IP address conflict records.

Syntax

display arp user-ip-conflict record [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays user IP address conflict records for all member devices.

Usage guidelines

Each IRF member device can save a maximum of 200 user IP address conflict records.

If the maximum number is reached, a new record will override the earliest record.

Examples

Display all user IP address conflict records.

```
<Sysname> display arp user-ip-conflict record
IP address: 10.1.1.1
System time: 2018-02-02 11:22:29
Conflict count: 1
Log suppress count: 0
Old interface: GigabitEthernet1/0/1
New interface: GigabitEthernet1/0/2
Old SVLAN/CVLAN: 100/2
New SVLAN/CVLAN: 100/2
Old MAC: 00e0-ca63-8141
New MAC: 00e0-ca63-8142

IP address: 10.1.1.2
System time: 2018-02-02 10:20:30
Conflict count: 1
Log suppress count: 0
Old interface: GigabitEthernet1/0/1
New interface: GigabitEthernet1/0/2
Old SVLAN/CVLAN: 100/--
New SVLAN/CVLAN: 100/--
Old MAC: 00e0-ca63-8141
New MAC: 00e0-ca63-8142
```

Table 2 Command output

Field	Description
IP address	IP address of a user.
System time	Time when the user IP address conflict occurred.
Conflict count	Number of times that conflicts for the IP address.
Log suppress count	Number of times that user IP address conflict logs are suppressed.
Old interface	Output interface in the old ARP entry.
New interface	Output interface in the new ARP entry.
Old SVLAN/CVLAN	ID of the outer VLAN or inner VLAN in the old ARP entry. This field displays hyphens (**--**) if the ARP entry does not belong to any outer VLAN or inner VLAN.
New SVLAN/CVLAN	ID of the outer VLAN or inner VLAN in the new ARP entry. This field displays hyphens (**--**) if the ARP entry does not belong to any outer VLAN or inner VLAN.
Old MAC	MAC address in the old ARP entry.
New MAC	MAC address in the new ARP entry.

Related commands

arp user-ip-conflict record enable

display arp user-move record

Use **display arp user-move record** to display user port migration records.

Syntax

display arp user-move record [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays user port migration records for all member devices.

Usage guidelines

Each IRF member device can save a maximum of 200 user port migration records.

When the number of user port migration records reaches the upper limit, new records will overwrite the earliest ones.

Examples

Display all user port migration records.

```
<Sysname> display arp user-move record
IP address: 10.1.1.1
MAC address: 0001-0201-0e81
System time: 2018-02-02 11:22:29
Move count: 1
Log suppress count: 0
Before:
  interface: GigabitEthernet1/0/1
  SVLAN/CVLAN: 100/2
After:
  interface: GigabitEthernet1/0/2
  SVLAN/CVLAN: 100/2

IP address: 10.1.1.2
MAC address: 0001-0201-0e82
System time: 2018-02-02 10:20:30
Move count: 1
Log suppress count: 0
Before:
  interface: GigabitEthernet1/0/1
  SVLAN/CVLAN: 100/--
After:
  interface: GigabitEthernet1/0/2
```

```
SVLAN/CVLAN: 100/--
```

Table 3 Command output

Field	Description
IP address	IP address of the user.
MAC address	MAC address of the user.
System time	Time when the user port migration occurred.
Move count	Number of times that user port migrated.
Log suppress count	Number of times that the generation of user port migration logs is suppressed.
Interface	Output interface in the ARP entry.
SVLAN/CVLAN	ID of the outer VLAN or inner VLAN in the ARP entry. This field displays hyphens (**--**) if the ARP entry does not belong to any outer VLAN or inner VLAN.

Related commands

arp user-move record enable

reset arp

Use **reset arp** to clear ARP entries from the ARP table.

Syntax

reset arp { **all** | **dynamic** | **interface** *interface-type interface-number* | **multiport** | **slot** *slot-number* | **static** }

Views

User view

Predefined user roles

network-admin

Parameters

all: Clears all ARP entries.

dynamic: Clears all dynamic ARP entries.

multiport: Clears all multiport ARP entries.

static: Clears all static ARP entries.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears ARP entries for the master device.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command clears ARP entries for all interfaces.

Usage guidelines

CAUTION:

The **reset arp** command will clear existing ARP entries from the ARP table. It might cause that external users cannot quickly communicate with the LAN users. Make sure you are fully aware of the impacts of this command when you use it on a live network.

Examples

Clear all static ARP entries.

```
<Sysname> reset arp static
```

Related commands

arp static

display arp

Gratuitous ARP commands

arp ip-conflict log prompt

Use **arp ip-conflict log prompt** to enable IP conflict notification.

Use **undo arp ip-conflict log prompt** to restore the default.

Syntax

arp ip-conflict log prompt

undo arp ip-conflict log prompt

Default

The default differs depending on the software version, as shown below:

Versions	Default setting
Versions earlier than Release 6350	IP conflict notification is disabled.
Release 6350 and later	• If the device starts up with the initial configuration, IP conflict notification is disabled. • If the device starts up with the factory defaults, IP conflict notification is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

By default, the device performs the following operations if it is using the sender IP address of a received ARP packet:

- Sends a gratuitous ARP request.
- Displays an error message after the device receives an ARP reply about the conflict.

You can use this command to enable the device to display error messages before sending a gratuitous ARP reply or request for conflict confirmation.

Examples

Enable IP conflict notification on the device.

```
<Sysname> system-view
[Sysname] arp ip-conflict log prompt
```

arp send-gratuitous-arp

Use **arp send-gratuitous-arp** to enable periodic sending of gratuitous ARP packets on an interface.

Use **undo arp send-gratuitous-arp** to disable the interface from periodically sending gratuitous ARP packets.

Syntax

arp send-gratuitous-arp [**interval** *interval*]

undo arp send-gratuitous-arp

Default

Periodic sending of gratuitous ARP packets is disabled.

Views

VLAN interface view

Predefined user roles

network-admin

Parameters

interval *interval*: Specifies the sending interval in the range of 200 to 200000 milliseconds. The default value is 2000 milliseconds.

Usage guidelines

This feature takes effect on an interface only when the interface has an IP address and the data link layer state of the interface is up.

This feature can send gratuitous ARP requests only for the sending interface's primary IP address or manually configured secondary IP address. The primary IP address can be configured manually or automatically, whereas the secondary IP address must be configured manually.

If you change the sending interval for gratuitous ARP packets, the configuration takes effect at the next sending interval.

The sending interval for gratuitous ARP packets might be much longer than the set interval when any of the following conditions exist:

- This feature is enabled on multiple interfaces.
- Each interface is configured with multiple secondary IP addresses.
- A small sending interval is configured in the preceding cases.

Examples

Enable VLAN-interface 2 to send gratuitous ARP packets every 300 milliseconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] arp send-gratuitous-arp interval 300
```

gratuitous-arp mac-change retransmit

Use **gratuitous-arp mac-change retransmit** to set the times and the interval for retransmitting a gratuitous ARP packet for the device MAC address change.

Use **undo gratuitous-arp mac-change retransmit** to restore the default.

Syntax

gratuitous-arp mac-change retransmit *times* **interval** *seconds*

undo gratuitous-arp mac-change retransmit

Default

The device sends a gratuitous packet for its MAC address change once only.

Views

System view

Predefined user roles

network-admin

Parameters

times: Specifies the times of retransmitting a gratuitous packet, in the range of 1 to 10.

interval *seconds*: Specifies the interval for retransmitting a gratuitous packet, in the range of 1 to 10 seconds.

Usage guidelines

The device sends a gratuitous ARP packet to inform other devices of its MAC address change. However, the other devices might fail to receive the packet because the device sends the gratuitous ARP packet once only by default. Use this command to configure gratuitous ARP retransmission parameters to ensure that the other devices can receive the packet.

After you execute this command, the device will retransmit a gratuitous ARP packet for its MAC address change at the specified interval for the specified times.

Examples

Set the times to 3 and the interval to 5 for retransmitting a gratuitous ARP packet for the device MAC address change.

```
<Sysname> system-view
[Sysname] gratuitous-arp mac-change retransmit 3 interval 5
```

gratuitous-arp-learning enable

Use **gratuitous-arp-learning enable** to enable learning of gratuitous ARP packets.

Use **undo gratuitous-arp-learning enable** to disable learning of gratuitous ARP packets.

Syntax

```
gratuitous-arp-learning enable
undo gratuitous-arp-learning enable
```

Default

Learning of gratuitous ARP packets is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The learning of gratuitous ARP packets feature allows a device to maintain its ARP table by creating or updating ARP entries based on received gratuitous ARP packets.

When this feature is disabled, the device uses received gratuitous ARP packets to update existing ARP entries only. ARP entries are not created based on the received gratuitous ARP packets, which saves ARP table space.

Examples

Enable learning of gratuitous ARP packets.

```
<Sysname> system-view
[Sysname] gratuitous-arp-learning enable
```

gratuitous-arp-sending enable

Use **gratuitous-arp-sending enable** to enable sending gratuitous ARP packets upon receiving ARP requests whose sender IP address is on a different subnet.

Use **undo gratuitous-arp-sending enable** to disable sending gratuitous ARP packets upon receiving ARP requests whose sender IP address is on a different subnet.

Syntax

gratuitous-arp-sending enable

undo gratuitous-arp-sending enable

Default

A device does not send gratuitous ARP packets when it receives ARP requests whose sender IP address is on a different subnet.

Views

System view

Predefined user roles

network-admin

Examples

Disable a device from sending gratuitous ARP packets upon receiving ARP requests whose sender IP address is on a different subnet.

```
<Sysname> system-view
[Sysname] undo gratuitous-arp-sending enable
```

Proxy ARP commands

display local-proxy-arp

Use **display local-proxy-arp** to display the local proxy ARP status.

Syntax

display local-proxy-arp [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays the local proxy ARP status for all interfaces.

Usage guidelines

You can use this command to check whether local proxy ARP is enabled or disabled.

Examples

Display the local proxy ARP status for VLAN-interface 2.

```
<Sysname> display local-proxy-arp interface vlan-interface 2
Interface Vlan-interface2
 Local Proxy ARP status: enabled
```

Related commands

local-proxy-arp enable

display proxy-arp

Use **display proxy-arp** to display the proxy ARP status.

Syntax

display proxy-arp [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays the proxy ARP status for all interfaces.

Usage guidelines

You can use this command to check whether proxy ARP is enabled or disabled.

Examples

Display the proxy ARP status on VLAN-interface 2.

```
<Sysname> display proxy-arp interface vlan-interface 2
Interface Vlan-interface2
 Proxy ARP status: disabled
```

Related commands

proxy-arp enable

local-proxy-arp enable

Use **local-proxy-arp enable** to enable local proxy ARP.

Use **undo local-proxy-arp enable** to disable local proxy ARP.

Syntax

local-proxy-arp enable [**ip-range** *start-ip-address* **to** *end-ip-address*]

undo local-proxy-arp enable

Default

Local proxy ARP is disabled.

Views

VLAN interface view

Predefined user roles

network-admin

Parameters

ip-range *start-ip-address* **to** *end-ip-address*: Specifies the IP address range for which local proxy ARP is enabled. The start IP address must be lower than or equal to the end IP address.

Usage guidelines

Proxy ARP enables a device on a network to answer ARP requests for an IP address not on that network. With proxy ARP, hosts in different broadcast domains can communicate with each other as they do on the same network.

Proxy ARP includes common proxy ARP and local proxy ARP.

Common proxy ARP allows communication between hosts that connect to different Layer 3 interfaces and reside in different broadcast domains.

Local proxy ARP allows communication between hosts that connect to the same Layer 3 interface and reside in different broadcast domains.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Enable local proxy ARP on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] local-proxy-arp enable
```

Enable local proxy ARP on VLAN-interface 2 for an IP address range.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] local-proxy-arp enable ip-range 1.1.1.1 to 1.1.1.20
```

Related commands

display local-proxy-arp

proxy-arp enable

Use **proxy-arp enable** to enable proxy ARP.

Use **undo proxy-arp enable** to disable proxy ARP.

Syntax

proxy-arp enable

undo proxy-arp enable

Default

Proxy ARP is disabled.

Views

VLAN interface view

Predefined user roles

network-admin

Usage guidelines

Proxy ARP enables a device on a network to answer ARP requests for an IP address not on that network. With proxy ARP, hosts in different broadcast domains can communicate with each other as they do on the same network.

Proxy ARP includes common proxy ARP and local proxy ARP.

Common proxy ARP allows communication between hosts that connect to different Layer 3 interfaces and reside in different broadcast domains.

Local proxy ARP allows communication between hosts that connect to the same Layer 3 interface and reside in different broadcast domains.

Examples

Enable proxy ARP on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] proxy-arp enable
```

Related commands

display proxy-arp

ARP snooping commands

arp snooping enable

Use **arp snooping enable** to enable ARP snooping.

Use **undo arp snooping enable** to disable ARP snooping.

Syntax

arp snooping enable

undo arp snooping enable

Default

ARP snooping is disabled.

Views

VLAN view

Predefined user roles

network-admin

Examples

Enable ARP snooping for VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] arp snooping enable
```

display arp snooping

Use **display arp snooping** to display ARP snooping entries.

Syntax

display arp snooping vlan [*vlan-id*]] [**slot** *slot-number*] [**count**]

display arp snooping vlan ip *ip-address* [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan: Displays ARP snooping entries for a VLAN.

vlan-id: Specifies a VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays ARP snooping entries for all VLANs.

count: Displays the number of the ARP snooping entries. If you do not specify this keyword, the command displays ARP snooping entries.

ip *ip-address*: Displays the ARP snooping entry for the specified IP address in VLANs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays ARP snooping entries for the master device.

Examples

Display ARP snooping entries for VLAN 2.

```
<Sysname> display arp snooping vlan 2
IP Address   MAC Address    VLAN ID Interface  Aging       Status
3.3.3.3         0003-0003-0003 2       GE1/0/1    20          Valid
3.3.3.4         0004-0004-0004 2       GE1/0/2    5           Invalid
```

Display the ARP snooping entry for IP address 1.1.1.1 in a VLAN.

```
<Sysname> display arp snooping vlan ip 1.1.1.1
IP address      MAC address    VLAN ID Interface  Aging       Status
1.1.1.1         001f-e201-0111 2       GE1/0/1    15          Valid
```

Table 4 Command output

Field	Description
IP Address	IP address in an ARP snooping entry.
MAC Address	MAC address in an ARP snooping entry.
VLAN ID	ID of the VLAN to which the ARP snooping entry belongs.
Interface	Input interface in an ARP snooping entry.
Aging	Aging time for an ARP snooping entry in minutes. If the member device learns an ARP snooping entry from another member, the member device cannot learn the aging time of the entry, and this field displays **N/A**.
Status	Status of an ARP snooping entry: **Valid**, **Invalid**, **Collision**.
Total entries	Number of ARP snooping entries.

Related commands

reset arp snooping

reset arp snooping

Use **reset arp snooping** to delete ARP snooping entries.

Syntax

reset arp snooping vlan [*vlan-id*]

reset arp snooping vlan ip *ip-address*

Views

User view

Predefined user roles

network-admin

Parameters

vlan: Deletes ARP snooping entries for a VLAN.

vlan-id: Specifies a VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command deletes ARP snooping entries for all VLANs.

ip *ip-address*: Deletes the ARP snooping entry for the specified IP address in VLANs.

Examples

Delete ARP snooping entries for VLAN 2.

```
<Sysname> reset arp snooping vlan 2
```

Related commands

display arp snooping

ARP direct route advertisement commands

arp route-direct advertise

Use **arp route-direct advertise** to enable ARP direct route advertisement.

Use **undo arp route-direct advertise** to disable ARP direct route advertisement.

Syntax

arp route-direct advertise

undo arp route-direct advertise

Default

ARP direct route advertisement is disabled.

Views

Interface view

Predefined user roles

network-admin

Examples

Enable ARP direct route advertisement on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] arp route-direct advertise
```

Contents

IP addressing commands

display ip interface

Use **display ip interface** to display IP configuration and statistics for Layer 3 interfaces.

Syntax

display ip interface [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays IP configuration and statistics for all Layer 3 interfaces.

Usage guidelines

Use the **display ip interface** command to display IP configuration and statistics for the specified Layer 3 interface. The statistics include the following information:

- The number of unicast packets, bytes, and multicast packets the interface has sent and received.
- The number of TTL-invalid packets and ICMP packets the interface has received.

The packet statistics helps you locate a possible attack on the network.

Examples

Display IP configuration and statistics for VLAN-interface 10.

```
<Sysname> display ip interface vlan-interface 10
Vlan-interface10 current state : DOWN
Line protocol current state : DOWN
Internet Address is 1.1.1.1/8 Primary
Broadcast address : 1.255.255.255
The Maximum Transmit Unit : 1500 bytes
input packets : 0, bytes : 0, multicasts : 0
output packets : 0, bytes : 0, multicasts : 0
TTL invalid packet number:         0
ICMP packet input number:          0
  Echo reply:                      0
  Unreachable:                     0
  Source quench:                   0
  Routing redirect:                0
  Echo request:                    0
  Router advert:                   0
  Router solicit:                  0
  Time exceed:                     0
```

```
IP header bad:                  0
Timestamp request:              0
Timestamp reply:                0
Information request:            0
Information reply:              0
Netmask request:                0
Netmask reply:                  0
Unknown type:                   0
```

Table 1 Command output

Field	Description
current state	Physical link state of the interface: • **Administrative DOWN**—The interface has been shut down by using the **shutdown** command. • **DOWN**—The interface is administratively up, but its physical state is down (possibly because no physical link exists or the link has failed). • **UP**—The interface is both administratively and physically up.
Line protocol current state	Data link layer state of the interface. • **DOWN**—The data link layer protocol is down. • **UP**—The data link layer protocol is up. • **UP (spoofing)**—The data link layer protocol is up, but the link is an on-demand link or does not exist.
Internet Address	IP address of an interface followed by: • **Primary**—A primary IP address. • **Sub**—A secondary IP address. • **Unnumbered**—An unnumbered IP address. • **DHCP-Allocated**—An IP address obtained through DHCP. • **BOOTP-Allocated**—An IP address obtained through BOOTP.
Broadcast address	Broadcast address of the subnet attached to an interface.
The Maximum Transmit Unit	MTU of the interface, in bytes.
input packets, bytes, multicasts output packets, bytes, multicasts	All received and sent packets and bytes, and received and sent multicast packets on an interface (statistics start at the device startup).
TTL invalid packet number	Number of TTL-invalid packets received on the interface (statistics start at the device startup).

Field	Description
ICMP packet input number: Echo reply: Unreachable: Source quench: Routing redirect: Echo request: Router advert: Router solicit: Time exceed: IP header bad: Timestamp request: Timestamp reply: Information request: Information reply: Netmask request: Netmask reply: Unknown type:	Total number of ICMP packets received on the interface (statistics start at the device startup): • Echo reply packets. • Unreachable packets. • Source quench packets. • Routing redirect packets. • Echo request packets. • Router advertisement packets. • Router solicitation packets. • Time exceeded packets. • IP header bad packets. • Timestamp request packets. • Timestamp reply packets. • Information request packets. • Information reply packets. • Netmask request packets. • Netmask reply packets. • Unknown type packets.

Related commands

display ip interface brief

ip address

display ip interface brief

Use **display ip interface brief** to display brief IP configuration for Layer 3 interfaces.

Syntax

display ip interface [*interface-type* [*interface-number*]] **brief** [**description**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type: Specifies an interface type. If you do not specify an interface type, this command displays brief IP configuration for all Layer 3 interfaces.

interface-number: Specifies an interface number. If you do not specify an interface number, this command displays brief IP configuration for all Layer 3 interfaces of the specified type.

description: Displays complete interface descriptions. If you do not specify this keyword, the command displays a maximum of 13 characters for each interface description. If the description is longer than 13 characters, the first 10 characters are displayed, followed by an ellipsis (...).

Usage guidelines

Information displayed by the command includes the state of the physical and link layer protocols, IP address, and interface descriptions.

Examples

Display brief IP configuration for VLAN interfaces.

```
<Sysname> display ip interface vlan-interface brief
*down: administratively down
(s): spoofing  (l): loopback
Interface           Physical Protocol IP address      VPN instance Description
Vlan10              down     down     6.6.6.1         --           Link to Co...
```

Display brief IP configuration for VLAN interfaces, including complete interface descriptions.

```
<Sysname> display ip interface vlan-interface brief description
*down: administratively down
(s): spoofing  (l): loopback
Interface           Physical Protocol IP address      VPN instance Description
Vlan10              down     down     6.6.6.1         --           Link to CoreR
                                                                   Outer
```

Table 2 Command output

Field	Description
*down: administratively down	The interface is administratively shut down by using the **shutdown** command.
(s) : spoofing	Spoofing attribute of the interface. The link protocol state of the interface is up, but the link is temporarily established on demand or does not exist.
Interface	Interface name.
Physical	Physical state of the interface: • ***down**—The interface is administratively shut down by using the **shutdown** command. • **down**—The interface is administratively up but its physical state is down, possibly because of a connection or link failure. • **up**—Both the administrative and physical states of the interface are up.
Protocol	Link layer protocol state of the interface: • **down**—The protocol state of the interface is down. • **down(l)**—The protocol state of the interface is down (loopback). • **up**—The protocol state of the interface is up. • **up(l)**—The protocol state of the interface is up (loopback). • **up(s)**—The protocol state of the interface is up (spoofing).
IP address	IP address of the interface. If no IP address is configured, this field displays hyphens (**--**).
VPN instance	This field is not supported in the current software version. Name of the VPN instance to which the interface belongs. This field displays a maximum of 12 characters. If the VPN instance name is longer than 12 characters, the first 9 characters are displayed, followed by an ellipsis (...). If the interface does not belong to any VPN instance, this field displays hyphens (**--**).
Description	Description of the interface. This field displays a maximum of 13 characters. If the description is longer than 13 characters, the first 10 characters are displayed, followed by an ellipsis (...). If no description is configured, this field displays hyphens (**--**).

Related commands

display ip interface

ip address

ip address

Use **ip address** to assign an IP address to the interface.

Use **undo ip address** to remove the IP address from the interface.

Syntax

ip address *ip-address* { *mask-length* | *mask* } [**irf-member** *member-id* | **sub**]

undo ip address *ip-address* { *mask-length* | *mask* } [**irf-member** *member-id* | **sub**]

Default

No IP address is assigned to an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address of the interface, in dotted decimal notation.

mask-length: Specifies the subnet mask length in the range of 1 to 31. For a loopback interface, the value range is 1 to 32.

mask: Specifies the subnet mask in dotted decimal notation.

irf-member *member-id*: Assigns an IP address to the management Ethernet port of the specified IRF member device. The *member-id* argument specifies an IRF member device by its member ID. The value range for the *member-id* argument is 1 to 10.

sub: Assigns a secondary IP address to the interface.

Usage guidelines

Use the command to assign a primary or secondary IP address to an interface.

An interface can have only one primary IP address. If you execute this command multiple times to specify different primary IP addresses on an interface, the most recent configuration takes effect. If the interface connects to multiple subnets, configure primary and secondary IP addresses on the interface so the subnets can communicate with each other through the interface.

You cannot assign secondary IP addresses to an interface that obtains an IP address through BOOTP IP unnumbered, or DHCP.

If you do not specify any parameters, the **undo ip address** command removes all IP addresses from the interface. The **undo ip address** *ip-address* { *mask* | *mask-length* } command removes the primary IP address. The **undo ip address** *ip-address* { *mask* | *mask-length* } **sub** command removes a secondary IP address.

The primary and secondary IP addresses assigned to the interface can be located on the same network segment. Different interfaces on your device must reside on different network segments.

If you assign IP addresses to the management Ethernet ports of IRF member devices, make sure the following requirements are met:

- The IP addresses must be in the same subnet if you assign them through the same management Ethernet port of the master device.
- The IP addresses must be in different subnets if you assign them through different management Ethernet ports of the master device.

In an IRF fabric, only the IP address assigned to the management Ethernet port of the master takes effect. Make sure no IP address conflict exists when you assign IP addresses to the management Ethernet ports of subordinates. The system does not warn of an IP address conflict because the IP addresses assigned to the management Ethernet ports of subordinates do not take effect. After an IRF fabric split, the IP addresses assigned to the management Ethernet ports of the new masters (original subordinates) take effect.

Examples

Assign VLAN-interface 10 a primary IP address 129.12.0.1 and a secondary IP address 202.38.160.1, with subnet masks both 255.255.255.0.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ip address 129.12.0.1 255.255.255.0
[Sysname-Vlan-interface10] ip address 202.38.160.1 255.255.255.0 sub
```

Related commands

display ip interface

display ip interface brief

ip address unnumbered

Use **ip address unnumbered** to configure the current interface as IP unnumbered to borrow an IP address from the specified interface.

Use **undo ip address unnumbered** to restore the default.

Syntax

ip address unnumbered interface *interface-type interface-number*

undo ip address unnumbered

Default

The interface does not borrow IP addresses from other interfaces.

Views

Interface view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface from which the current interface can borrow an IP address.

Usage guidelines

Typically, you assign an IP address to an interface either manually or through DHCP. If the IP addresses are not enough, or the interface is used only occasionally, you can configure an interface to borrow an IP address from other interfaces. This is called IP unnumbered, and the interface borrowing the IP address is called IP unnumbered interface.

Loopback interfaces cannot borrow IP addresses of other interfaces, but other interfaces can borrow IP addresses of loopback interfaces.

Multiple interfaces can use the same unnumbered IP address. If an interface has multiple manually configured IP addresses, only the primary IP address manually configured can be borrowed.

You cannot enable a dynamic routing protocol on the interface that has no IP address configured. To enable the interface to communicate with other devices, you must configure a static route to the peer device on the interface.

Examples

Configure VLAN-interface 10 to borrow the IP address of VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ip address unnumbered interface vlan-interface 100
```

Contents

DHCP commands

Common DHCP commands

dhcp client-detect

Use **dhcp client-detect** to enable client offline detection on the DHCP server or DHCP relay agent.

Use **undo dhcp client-detect** to disable client offline detection on the DHCP server or DHCP relay agent.

Syntax

dhcp client-detect

undo dhcp client-detect

Default

Client offline detection is disabled on the DHCP server or DHCP relay agent.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

The client offline detection feature on the DHCP server reclaims an assigned IP address and deletes the binding entry when the ARP entry ages out for the IP address.

This feature on the DHCP relay agent deletes the related relay entry and sends a RELEASE message to the DHCP server when an ARP entry ages out.

Examples

Enable client offline detection.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp client-detect
```

dhcp dscp

Use **dhcp dscp** to set the DSCP value for DHCP packets sent by the DHCP server or the DHCP relay agent.

Use **undo dhcp dscp** to restore the default.

Syntax

dhcp dscp *dscp-value*

undo dhcp dscp

Default

The DSCP value is 56 in DHCP packets sent by the DHCP server or the DHCP relay agent.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies the DSCP value for DHCP packets, in the range of 0 to 63.

Usage guidelines

The DSCP value of a packet specifies the priority level of the packet and affects the transmission priority of the packet. A bigger DSCP value represents a higher priority.

Examples

Set the DSCP value to 30 for DHCP packets sent by the DHCP server or the DHCP relay agent.

```
<Sysname> system-view
[Sysname] dhcp dscp 30
```

dhcp enable

Use **dhcp enable** to enable DHCP.

Use **undo dhcp enable** to disable DHCP.

Syntax

dhcp enable

undo dhcp enable

Default

DHCP is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

DHCP related configuration takes effect only after you enable DHCP.

Enable DHCP before you configure the DHCP server or relay agent.

Examples

Enable DHCP.

```
<Sysname> system-view
[Sysname] dhcp enable
```

dhcp log enable

Use **dhcp log enable** to enable DHCP server logging.

Use **undo dhcp log enable** to disable DHCP server logging.

Syntax

dhcp log enable

undo dhcp log enable

Default

DHCP server logging is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command enables the DHCP server to generate DHCP logs and send them to the information center. The information helps administrators to locate and solve problems. For information about the log destination and output rule configuration in the information center, see *Network Management and Monitoring Configuration Guide*.

As a best practice, disable this feature if the log generation affects the device performance or reduces the address allocation efficiency. For example, this situation might occur when a large number of clients frequently come online or go offline.

Examples

Enable DHCP server logging.

```
<Sysname> system-view
[Sysname] dhcp log enable
```

dhcp select

Use **dhcp select** to enable the DHCP server or DHCP relay agent on an interface.

Use **undo dhcp select** to disable the DHCP server or DHCP relay agent on an interface. The interface will discard incoming DHCP packets.

Syntax

dhcp select { **relay** [**proxy**] | **server** }

undo dhcp select { **relay** | **server** }

Default

The interface operates in the DHCP server mode and responds to DHCP requests with configuration parameters.

Views

Interface view

Predefined user roles

network-admin

Parameters

relay: Enables the DHCP relay agent on the interface.

proxy: Enables the DHCP server proxy on the relay agent.

server: Enables the DHCP server on the interface.

Usage guidelines

Before enabling a DHCP server to operate as a DHCP relay agent, use the **reset dhcp server ip-in-use** command to clear address bindings and authorized ARP entries. These authorized ARP entries might conflict with ARP entries that are created after the DHCP relay agent is enabled.

When DHCP server proxy is enabled on the DHCP relay agent, the proxy forwards packets between the DHCP clients and DHCP server.

- When receiving DHCP requests from DHCP clients, the proxy forwards them to the DHCP server.
- When receiving DHCP responses from the DHCP server, the proxy modifies the DHCP server's IP address in these responses as its own IP address.

Examples

Enable the DHCP relay agent on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] dhcp select relay
```

Related commands

dhcp relay server-address

dhcp relay source-address

dhcp server request-ip-address check

dhcp smart-relay enable

reset dhcp server ip-in-use

DHCP server commands

NOTE:

- S5110V2-SI, S5000V3-EI, S5000E-X, S5000X-EI, and WAS6000 do not support the DHCP server functionality.
- S5000V5-EI supports the DHCP server functionality as from Release 6328P02 and Release 6337.

address range

Use **address range** to configure an IP address range in a DHCP address pool for dynamic allocation.

Use **undo address range** to restore the default.

Syntax

address range *start-ip-address end-ip-address*

undo address range

Default

No IP address range exists.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

start-ip-address: Specifies the start IP address.

end-ip-address: Specifies the end IP address.

Usage guidelines

If no IP address range is specified, all IP addresses in the subnet specified by the **network** command in address pool view are assignable. If an IP address range is specified, only the IP addresses in the IP address range are assignable.

After you use the **address range** command, you cannot use the **network secondary** command to specify a secondary subnet in the address pool.

If you execute this command multiple times, the most recent configuration takes effect.

The address range specified by the **address range** command must be within the subnet specified by the **network** command. The addresses outside of the subnet cannot be assigned.

Examples

Specify an address range of 192.168.8.1 through 192.168.8.150 in address pool 1.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 1
[Sysname-dhcp-pool-1] address range 192.168.8.1 192.168.8.150
```

Related commands

class

dhcp class

display dhcp server pool

network

bims-server

Use **bims-server** to specify the IP address, port number, and shared key of the BIMS server in a DHCP address pool.

Use **undo bims-server** to restore the default.

Syntax

bims-server ip *ip-address* [**port** *port-number*] **sharekey** { **cipher** | **simple** } *string*

undo bims-server

Default

No BIMS server information is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

ip *ip-address*: Specifies the IP address of the BIMS server.

port *port-number*: Specifies the port number of the BIMS server, in the range of 1 to 65534.

cipher: Specifies a key in encrypted form.

simple: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key string. Its plaintext form is a case-sensitive string of 1 to 16 characters. Its encrypted form is a case-sensitive string of 1 to 53 characters. The DHCP client uses the shared key to encrypt packets sent to the BIMS server.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify BIMS server IP address 1.1.1.1, port number 80, and shared key **aabbcc** in address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] bims-server ip 1.1.1.1 port 80 sharekey simple aabbcc
```

Related commands

display dhcp server pool

bootfile-name

Use **bootfile-name** to specify a configuration file name or URL.

Use **undo bootfile-name** to restore the default.

Syntax

bootfile-name { *bootfile-name* | *url* }

undo bootfile-name

Default

No configuration file name or URL is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

bootfile-name: Specifies the configuration file name, a case-sensitive string of 1 to 63 characters.

url: Specifies the HTTP URL of the configuration file. It is a case-sensitive string of 1 to 63 characters.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

To specify a configuration file on a TFTP server, use the *bootfile-name* argument.

To specify a configuration file on an HTTP server, use the *url* argument.

Examples

Specify configuration file name **boot.cfg** in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] bootfile-name boot.cfg
```

Specify configuration file URL **http://10.1.1.1/boot.cfg** in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] bootfile-name http://10.1.1.1/boot.cfg
```

Related commands

display dhcp server pool

next-server

tftp-server domain-name

tftp-server ip-address

class ip-pool

Use **class ip-pool** to specify a DHCP address pool for a DHCP user class.

Use **undo class ip-pool** to remove the DHCP address pool specified for a DHCP user class.

Syntax

class *class-name* **ip-pool** *pool-name*

undo class *class-name* **ip-pool**

Default

No DHCP address pool is specified for a DHCP user class.

Views

DHCP policy view

Predefined user roles

network-admin

Parameters

class-name: Specifies a DHCP user class by its name, a case-insensitive string of 1 to 63 characters.

pool-name: Specifies a DHCP address pool by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can specify only one DHCP address pool for a DHCP user class in a DHCP policy. If you execute this command multiple times for a user class, the most recent configuration takes effect.

Examples

Specify DHCP address pool **pool1** for DHCP user class **test** in DHCP policy 1.

```
<Sysname> system-view
[Sysname] dhcp policy 1
[Sysname-dhcp-policy-1] class test ip-pool pool1
```

Related commands

default ip-pool

dhcp policy

dhcp server ip-pool

class option-group

Use **class option-group** to specify a DHCP option group for a DHCP user class.

Use **undo class option-group** to remove the configuration.

Syntax

class *class-name* **option-group** *option-group-number*

undo class *class-name* **option-group**

Default

No DHCP option group is specified for a DHCP user class.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

class-name: Specifies a DHCP user class by its name, a case-insensitive string of 1 to 63 characters.

option-group-number: Specifies a DHCP option group by its number in the range of 1 to 32768.

Usage guidelines

When receiving a DHCP-DISCOVER message, the server compares the client against the user classes in the order that they are specified by this command. If a match is found, the server assigns the client the DHCP options in the option group. If multiple matches are found, the server selects option groups by using the following methods:

- If the option groups have options in common, the server selects the option group specified for the first matching user class.
- If the option groups have different options, the server selects all the matching option groups.

You can specify only one option group for a DHCP user class in a DHCP address pool. If you execute this command multiple times for a user class, the most recent configuration takes effect.

Examples

Specify DHCP option group 1 for user class **user** in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] class user option-group 1
```

Related commands

dhcp option-group

class range

Use **class range** to specify an IP address range for a DHCP user class.

Use **undo class range** to remove the IP address range for the DHCP user class.

Syntax

class *class-name* **range** *start-ip-address end-ip-address*

undo class *class-name* **range**

Default

No IP address range is specified for a DHCP user class.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

class-name: Specifies a DHCP user class name, a case-insensitive string of 1 to 63 characters. If the specified user class does not exist, the DHCP server will not assign the addresses in the address range specified for the user class to any clients.

start-ip-address: Specifies the start IP address.

end-ip-address: Specifies the end IP address.

Usage guidelines

The **class range** command allows you to divide an address range into multiple address ranges for different DHCP user classes. The address range for a user class must be within the primary subnet specified by the **network** command. If the DHCP client does not match any DHCP user class, the DHCP server selects an address in the IP address range specified by the **address range** command. If the address range has no assignable IP addresses or no address range is configured, the address allocation fails.

After you specify an address range for a user class, you cannot use the **network secondary** command to specify a secondary subnet in the address pool.

You can specify only one address range for a DHCP user class in an address pool. If you execute this command multiple times for a DHCP user class, the most recent configuration takes effect.

Examples

Specify an IP address range of 192.168.8.1 through 192.168.8.150 for DHCP user class **user** in DHCP address pool 1.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 1
[Sysname-dhcp-pool-1] class user range 192.168.8.1 192.168.8.150
```

Related commands

address range

dhcp class

display dhcp server pool

default ip-pool

Use **default ip-pool** to specify the default DHCP address pool.

Use **undo default ip-pool** to restore the default.

Syntax

default ip-pool *pool-name*

undo default ip-pool

Default

No default DHCP address pool is specified.

Views

DHCP policy view

Predefined user roles

network-admin

Parameters

pool-name: Specifies a DHCP address pool by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

In a DHCP policy, the DHCP server uses the default DHCP address pool to assign IP addresses and other parameters to clients that do not match any user classes. If no default address pool is specified or the default address pool does not have assignable IP addresses, the address assignment fails.

You can specify only one default address pool in a DHCP policy. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify DHCP address pool **pool1** as the default DHCP address pool in DHCP policy 1.

```
<Sysname> system-view
[Sysname] dhcp policy 1
[Sysname-dhcp-policy-1] default ip-pool pool1
```

Related commands

class ip-pool

dhcp policy

dhcp apply-policy

Use **dhcp apply-policy** to apply a DHCP policy to an interface.

Use **undo dhcp apply-policy** to restore the default.

Syntax

dhcp apply-policy *policy-name*

undo dhcp apply-policy

Default

No DHCP policy is applied to an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a DHCP policy by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can apply only one DHCP policy to an interface. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Apply DHCP policy **test** to VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp apply-policy test
```

Related commands

dhcp policy

dhcp class

Use **dhcp class** to create a DHCP user class and enter its view, or enter the view of an existing DHCP user class.

Use **undo dhcp class** to delete the specified DHCP user class.

Syntax

dhcp class *class-name*

undo dhcp class *class-name*

Default

No DHCP user classes exist.

Views

System view

Predefined user roles

network-admin

Parameters

class-name: Specifies the name of a DHCP user class, a case-insensitive string of 1 to 63 characters.

Usage guidelines

In the DHCP user class view, you can use the **if-match** command to configure match rules to group clients to the user class.

Examples

Create DHCP user class **test** and enter DHCP user class view.

```
<Sysname> system-view
[Sysname] dhcp class test
[Sysname-dhcp-class-test]
```

Related commands

address range

class ip-pool

class option-group

class range

dhcp policy

if-match

dhcp option-group

Use **dhcp option-group** to create a DHCP option group and enter its view, or enter the view of an existing DHCP option group.

Use **undo dhcp option-group** to delete a DHCP option group.

Syntax

dhcp option-group *option-group-number*

undo dhcp option-group *option-group-number*

Default

No DHCP option groups exist.

Views

System view

Predefined user roles

network-admin

Parameters

option-group-number: Assigns a number to the DHCP option group, in the range of 1 to 32768.

Examples

Create DHCP option group 1 and enter DHCP option group view.

```
<Sysname> system-view
[Sysname] dhcp option-group 1
[Sysname-dhcp-option-group-1]
```

Related commands

class option-group

option

dhcp policy

Use **dhcp policy** to create a DHCP policy and enter its view, or enter the view of an existing DHCP policy.

Use **undo dhcp policy** to delete a DHCP policy.

Syntax

dhcp policy *policy-name*

undo dhcp policy *policy-name*

Default

No DHCP policies exist.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Assigns a name to the DHCP policy. The policy name is a case-insensitive string of 1 to 63 characters.

Usage guidelines

In DHCP policy view, you can specify address pools for different user classes. Clients matching a user class will obtain IP addresses and other parameters from the specified address pool.

For a DHCP policy to take effect, you must apply it to an interface.

Examples

Create DHCP policy **test** and enter its view.

```
<Sysname> system-view
[Sysname] dhcp policy test
[Sysname-dhcp-policy-test]
```

Related commands

class ip-pool

default ip-pool

dhcp apply-policy

dhcp class

dhcp server always-broadcast

Use **dhcp server always-broadcast** to enable the DHCP server to broadcast all responses.

Use **undo dhcp server always-broadcast** to restore the default.

Syntax

dhcp server always-broadcast

undo dhcp server always-broadcast

Default

The DHCP server reads the broadcast flag in a DHCP request to decide whether to broadcast or unicast the response.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command enables the DHCP server to ignore the broadcast flag in DHCP requests and broadcast all responses.

The DHCP server always unicasts a response in the following situations, regardless of whether this command is executed:

- The DHCP request is from a DHCP client that has an IP address (the **ciaddr** field is not 0).
- The DHCP request is forwarded by a DHCP relay agent from a DHCP client (the **giaddr** field is not 0).

Examples

Enable the DHCP server to broadcast all responses.

```
<Sysname> system-view
[Sysname] dhcp server always-broadcast
```

dhcp server apply ip-pool

Use **dhcp server apply ip-pool** to apply an address pool to an interface.

Use **undo dhcp server apply ip-pool** to restore the default.

Syntax

dhcp server apply ip-pool *pool-name*

undo dhcp server apply ip-pool

Default

No address pool is applied to an interface

Views

Interface view

Predefined user roles

network-admin

Parameters

pool-name: Specifies the name of a DHCP address pool, a case-insensitive string of 1 to 63 characters.

Usage guidelines

Upon receiving a DHCP request from the interface, the DHCP server searches for a static binding for the client from all address pools. If no static binding is found, the server assigns configuration parameters from the address pool applied on the interface to the client. If the address pool has no assignable IP address or does not exist, the DHCP client cannot obtain an IP address.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Apply DHCP address pool 0 to VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] dhcp server apply ip-pool 0
```

Related commands

dhcp server ip-pool

dhcp server bootp ignore

Use **dhcp server bootp ignore** to configure the DHCP server to ignore BOOTP requests.

Use **undo dhcp server bootp ignore** to restore the default.

Syntax

dhcp server bootp ignore

undo dhcp server bootp ignore

Default

The DHCP server does not ignore BOOTP requests.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The lease duration of IP addresses obtained by BOOTP clients is unlimited. For scenarios that do not allow unlimited leases, you can configure the DHCP server to ignore BOOTP requests.

Examples

Configure the DHCP server to ignore BOOTP requests.

```
<Sysname> system-view
[Sysname] dhcp server bootp ignore
```

dhcp server bootp reply-rfc-1048

Use **dhcp server bootp reply-rfc-1048** to enable the sending of BOOTP responses in RFC 1048 format.

Use **undo dhcp server bootp reply-rfc-1048** to disable this feature.

Syntax

dhcp server bootp reply-rfc-1048

undo dhcp server bootp reply-rfc-1048

Default

This feature is disabled. The DHCP server does not process the Vend field of RFC 1048-incompliant requests but copies the Vend field into responses.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Not all BOOTP clients can send requests compliant with RFC 1048. This command enables the DHCP server to fill the Vend field in RFC 1048-compliant format in DHCP responses to RFC 1048-incompliant requests sent by BOOTP clients.

Examples

Enable the sending of BOOTP responses in RFC 1048 format on the DHCP server.

```
<Sysname> system-view
[Sysname] dhcp server bootp reply-rfc-1048
```

dhcp server check mac-address

Use **dhcp server check mac-address** to enable MAC address check on the DHCP server.

Use **undo dhcp server check mac-address** to disable MAC address check on the DHCP server.

Syntax

dhcp server check mac-address

undo dhcp server check mac-address

Default

MAC address check is disabled on the DHCP server.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

This feature enables the DHCP server to compare the **chaddr** field of a received DHCP request with the source MAC address in the frame header. If they are the same, the DHCP server verifies the packet as legal and continues processing the packet. If they are not the same, the DHCP server discards the request.

Examples

Enable MAC address check on the DHCP server.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp server check mac-address
```

dhcp server database filename

Use **dhcp server database filename** to configure the DHCP server to back up the DHCP bindings to a file.

Use **undo dhcp server database filename** to restore the default.

Syntax

dhcp server database filename { *filename* | **url** *url* [**username** *username* [**password** { **cipher** | **simple** } *string*]] }

undo dhcp server database filename

Default

The DHCP server does not back up the DHCP bindings.

Views

System view

Predefined user roles

network-admin

Parameters

filename: Specifies the name of a local backup file. For information about the *filename* argument, see *Fundamentals Configuration Guide*.

url *url*: Specifies the URL of a remote backup file, a case-sensitive string of 1 to 255 characters. Do not include a username or password in the URL.

username *username*: Specifies the username for accessing the URL of the remote backup file, a case-sensitive string of 1 to 32 characters. Do not specify this option if a username is not required for accessing the URL of the remote backup file.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 32 characters. Its encrypted form is a case-sensitive string of 1 to 73 characters. Do not specify this argument if a password is not required for accessing the URL of the remote backup file.

Usage guidelines

The command automatically creates the file if you specify a nonexistent file.

With this command executed, the DHCP server backs up its bindings immediately and runs auto backup. The server, by default, waits 300 seconds after a binding change to update the backup file. You can use the **dhcp server database update interval** command to change the waiting time. If no DHCP binding changes, the backup file is not updated.

As a best practice, back up the bindings to a remote file. If you use the local storage medium, the frequent erasing and writing might damage the medium and then cause the DHCP server to malfunction.

When the backup file is on a remote device, follow these restrictions and guidelines to specify the URL, username, and password:

If the file is on an FTP server, enter URL in the following format: ftp://*server address:port/file path*, where the port number is optional.

If the file is on a TFTP server, enter URL in the following format: tftp://*server address:port/file path*, where the port number is optional.

- The username and password must be the same as those configured on the FTP server. If the server authenticates only the username, the password can be omitted.
- If the IP address of the server is an IPv6 address, enclose the address in a pair of brackets, for example, **ftp://[1::1]/database.dhcp**.
- You can also specify the DNS domain name for the server address field, for example, **ftp://company/database.dhcp**.

Examples

Configure the DHCP server to back up its bindings to file **database.dhcp**.

```
<Sysname> system-view
[Sysname] dhcp server database filename database.dhcp
```

Configure the DHCP server to back up its bindings to file **database.dhcp** in the working directory of the FTP server at 10.1.1.1.

```
<Sysname> system-view
[Sysname] dhcp server database filename url ftp://10.1.1.1/database.dhcp username 1
password simple 1
```

Related commands

dhcp server database update interval

dhcp server database update now

dhcp server database update stop

dhcp server database update interval

Use **dhcp server database update interval** to set the waiting time for the DHCP server to update the backup file after a DHCP binding change.

Use **undo dhcp server database update interval** to restore the default.

Syntax

dhcp server database update interval *interval*

undo dhcp server database update interval

Default

The DHCP server waits 300 seconds to update the backup file after a DHCP binding change. If no DHCP binding changes, the backup file is not updated.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the waiting time in the range of 60 to 864000 seconds.

Usage guidelines

When a DHCP binding is created, updated, or removed, the waiting period starts. The DHCP server updates the backup file when the waiting period is reached. All bindings changed during the period will be saved to the backup file.

The waiting time takes effect only after you configure the DHCP binding auto backup by using the **dhcp server database filename** command.

Examples

Set the waiting time to 10 minutes for the DHCP server to update the backup file.

```
<Sysname> system-view
[Sysname] dhcp server database update interval 600
```

Related commands

dhcp server database filename

dhcp server database update now

dhcp server database update stop

dhcp server database update now

Use **dhcp server database update now** to manually save the DHCP bindings to the backup file.

Syntax

dhcp server database update now

Views

System view

Predefined user roles

network-admin

Usage guidelines

Each time this command is executed, the DHCP bindings are saved to the backup file.

For this command to take effect, you must configure the DHCP auto backup by using the **dhcp server database filename** command.

Examples

Manually save the DHCP bindings to the backup file.

```
<Sysname> system-view
[Sysname] dhcp server database update now
```

Related commands

dhcp server database filename

dhcp server database update interval

dhcp server database update stop

dhcp server database update stop

Use **dhcp server database update stop** to terminate the download of DHCP bindings from the backup file.

Syntax

dhcp server database update stop

Views

System view

Predefined user roles

network-admin

Usage guidelines

The DHCP server does not provide services during the binding download process. If the connection disconnects during the process, the waiting timeout timer is 60 minutes. When the timer expires, the DHCP server stops waiting and starts providing address allocation services.

To enable the DHCP server to provide services without waiting for the connection to be repaired, use this command to terminate the download immediately. The IP addresses associated with the undownloaded bindings will be assigned to clients. Address conflicts might occur.

Examples

Terminate the download of the backup DHCP bindings.

```
<Sysname> system-view
[Sysname] dhcp server database update stop
```

Related commands

dhcp server database filename

dhcp server database update interval

dhcp server database update now

dhcp server forbidden-ip

Use **dhcp server forbidden-ip** to exclude IP addresses from dynamic allocation globally.

Use **undo dhcp server forbidden-ip** to remove the configuration.

Syntax

dhcp server forbidden-ip *start-ip-address* [*end-ip-address*]

undo dhcp server forbidden-ip *start-ip-address* [*end-ip-address*]

Default

No IP addresses are excluded from dynamic allocation globally.

Views

System view

Predefined user roles

network-admin

Parameters

start-ip-address: Specifies the start IP address.

end-ip-address: Specifies the end IP address, which cannot be lower than the *start-ip-address*. If you do not specify this argument, only the *start-ip-address* is excluded from dynamic allocation.

Usage guidelines

The IP addresses of some devices such as the gateway and FTP server cannot be assigned to clients. Use this command to exclude such addresses from dynamic allocation.

If the excluded IP address is in a static DHCP binding, the address can still be assigned to the client.

The address or address range specified in the **undo dhcp server forbidden-ip** command must be the same as that specified in the **dhcp server forbidden-ip** command. To remove an IP address from the specified address range, you must remove the entire address range.

You can execute this command multiple times to exclude multiple IP address ranges from dynamic allocation.

Examples

Exclude the IP addresses of 10.110.1.1 through 10.110.1.63 from dynamic allocation globally.

```
<Sysname> system-view
[Sysname] dhcp server forbidden-ip 10.110.1.1 10.110.1.63
```

Related commands

forbidden-ip

static-bind

dhcp server ip-pool

Use **dhcp server ip-pool** to create a DHCP address pool and enter its view, or enter the view of an existing DHCP address pool.

Use **undo dhcp server ip-pool** to delete the specified DHCP address pool.

Syntax

dhcp server ip-pool *pool-name*

undo dhcp server ip-pool *pool-name*

Default

No DHCP address pools exist.

Views

System view

Predefined user roles

network-admin

Parameters

pool-name: Specifies a DHCP address pool name, a case-insensitive string of 1 to 63 characters. The pool name uniquely identifies an address pool.

Usage guidelines

A DHCP address pool is used to store the configuration parameters to be assigned to DHCP clients.

Examples

Create a DHCP address pool named **pool1**.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool pool1
[Sysname-dhcp-pool-pool1]
```

Related commands

class ip-pool

dhcp server apply ip-pool

display dhcp server pool

dhcp server ping packets

Use **dhcp server ping packets** to set the maximum number of ping packets.

Use **undo dhcp server ping packets** to restore the default.

Syntax

dhcp server ping packets *number*

undo dhcp server ping packets

Default

The maximum number of ping packets is 1.

Views

System view

Predefined user roles

network-admin

Parameters

number: Sets the maximum number of ping packets, in the range of 0 to 10. To disable the address conflict detection, set the value to 0.

Usage guidelines

To avoid IP address conflicts, the DHCP server pings an IP address before assigning it to a DHCP client.

If a ping attempt succeeds, the server determines that the IP address is in use and picks a new IP address. If all the ping attempts fail, the server assigns the IP address to the requesting DHCP client.

Examples

Set the maximum number of ping packets to 10.

```
<Sysname> system-view
[Sysname] dhcp server ping packets 10
```

Related commands

dhcp server ping timeout

display dhcp server conflict

reset dhcp server conflict

dhcp server ping timeout

Use **dhcp server ping timeout** to set the ping response timeout time on the DHCP server.

Use **undo dhcp server ping timeout** to restore the default.

Syntax

dhcp server ping timeout *milliseconds*

undo dhcp server ping timeout

Default

The ping response timeout time is 500 milliseconds.

Views

System view

Predefined user roles

network-admin

Parameters

milliseconds: Specifies the timeout time in the range of 0 to 10000 milliseconds. To disable the ping operation for address conflict detection, set the value to 0 milliseconds.

Usage guidelines

To avoid IP address conflicts, the DHCP server pings an IP address before assigning it to a DHCP client.

If a ping attempt succeeds, the server determines that the IP address is in use and picks a new IP address. If all the ping attempts fail, the server assigns the IP address to the requesting DHCP client.

Examples

Set the response timeout time to 1000 milliseconds.

```
<Sysname> system-view
[Sysname] dhcp server ping timeout 1000
```

Related commands

dhcp server ping packets

display dhcp server conflict

reset dhcp server conflict

dhcp server relay information enable

Use **dhcp server relay information enable** to enable the DHCP server to handle Option 82.

Use **undo dhcp server relay information enable** to configure the DHCP server to ignore Option 82.

Syntax

dhcp server relay information enable

undo dhcp server relay information enable

Default

The DHCP server handles Option 82.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Upon receiving a DHCP request that contains Option 82, the server copies the original Option 82 into the response. If the server is configured to ignore Option 82, the response will not contain Option 82.

Examples

Configure the DHCP server to ignore Option 82.

```
<Sysname> system-view
[Sysname] undo dhcp server relay information enable
```

dhcp server request-ip-address check

Use **dhcp server request-ip-address check** to enable the DHCP server to return a DHCP-NAK message if the client notions of their IP addresses are incorrect.

Use **undo dhcp server request-ip-address check** to restore the default.

Syntax

dhcp server request-ip-address check

undo dhcp server request-ip-address check

Default

The DHCP server does not return a DHCP-NAK message if the client notions of their IP addresses are incorrect.

Views

System view

Predefined user roles

network-admin

Usage guidelines

A DHCP client can send a DHCP-REQUEST message directly or upon receiving a DHCP-OFFER message. Upon receiving the request, the DHCP server will check if the client notion of its IP address is correct. If the requested IP address is different from the allocated one or has no matching lease

record, the DHCP server remains silent by default. After the allocated IP address lease for the client expires, the DHCP server will make response to request from the client.

This feature enables the DHCP server to return DHCP-NAK messages if the client notions of their IP addresses are incorrect. After receiving the DHCP-NAK message, the DHCP client will request an IP address again.

Examples

Enable the DHCP server to return a DHCP-NAK message if the client notions of their IP addresses are incorrect.

```
<Sysname> system-view
[Sysname] dhcp server request-ip-address check
```

Related commands

dhcp select server

display dhcp server conflict

Use **display dhcp server conflict** to display information about IP address conflicts.

Syntax

display dhcp server conflict [**ip** *ip-address*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ip *ip-address*: Displays conflict information about the specified IP address. If you do not specify this option, this command displays information about all IP address conflicts.

Usage guidelines

The DHCP server generates IP address conflict information in the following situations:

- Before assigning an IP address to a DHCP client, the DHCP server pings the IP address and discovers that another host is using the address.
- The DHCP client sends a DECLINE packet to the DHCP server to inform the server of an IP address conflict.
- The DHCP server discovers that the only assignable address in the address pool is its own IP address.

Examples

Display information about all IP address conflicts.

```
<Sysname> display dhcp server conflict
IP address          Detect time
4.4.4.1             Apr 25 16:57:20 2007
4.4.4.2             Apr 25 17:00:10 2007
```

Table 1 Command output

Field	Description
IP address	Conflicted IP address.

Field	Description
Detect time	Time when the conflict was discovered.

Related commands

`reset dhcp server conflict`

display dhcp server database

Use **`display dhcp server database`** to display information about DHCP binding auto backup.

Syntax

`display dhcp server database`

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display information about DHCP binding auto backup.

```
<Sysname> display dhcp server database
 File name               :   database.dhcp
 Username                :
 Password                :
 Update interval         :   600 seconds
 Latest write time       :   Feb  8 16:09:53 2014
 Status                  :   Last write succeeded.
```

Table 2 Command output

Field	Description
File name	Name of the DHCP binding backup file.
Username	Username for accessing the URL of the remote backup file.
Password	Password for accessing the URL of the remote backup file. This field displays ********** if a password is configured.
Update interval	Waiting time in seconds after a DHCP binding change for the DHCP server to update the backup file.
Latest write time	Time of the latest update.
Status	Status of the update: • **Writing**—The backup file is being updated. • **Last write succeeded**—The backup file was successfully updated. • **Last write failed**—The backup file failed to be updated.

display dhcp server expired

Use **`display dhcp server expired`** to display the lease expiration information.

Syntax

display dhcp server expired [**ip** *ip-address* | **pool** *pool-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ip *ip-address*: Displays lease expiration information about the specified IP address. If you do not specify an IP address, this command displays lease expiration information about all IP addresses.

pool *pool-name*: Displays lease expiration information about the specified address pool. The pool name is a case-insensitive string of 1 to 63 characters. If you do not specify an address pool, this command displays lease expiration information about all address pools.

Usage guidelines

DHCP assigns these expired IP addresses to DHCP clients when all available addresses have been assigned.

Examples

Display all lease expiration information.

```
<Sysname> display dhcp server expired
IP address       Client-identifier/Hardware address    Lease expiration
4.4.4.6          3030-3066-2e65-3230-302e-3130-3234    Apr 25 17:10:47 2007
                 -2d45-7468-6572-6e65-7430-2f31
```

Table 3 Command output

Field	Description
IP address	Expired IP address.
Client-identifier/Hardware address	Client ID or MAC address.
Lease expiration	Time when the lease expired.

Related commands

reset dhcp server expired

display dhcp server free-ip

Use **display dhcp server free-ip** to display information about assignable IP addresses.

Syntax

display dhcp server free-ip [**pool** *pool-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

pool *pool-name*: Displays assignable IP addresses in the specified address pool. The pool name is a case-insensitive string of 1 to 63 characters. If you do not specify an address pool, this command displays all assignable IP addresses for all address pools.

Examples

Display assignable IP addresses in all address pools.

```
<Sysname> display dhcp server free-ip
Pool name: 1
  Network: 10.0.0.0 mask 255.0.0.0
    IP ranges from 10.0.0.10 to 10.0.0.100
    IP ranges from 10.0.0.105 to 10.0.0.255
  Secondary networks:
    10.1.0.0 mask 255.255.0.0
      IP ranges from 10.1.0.0 to 10.1.0.255
    10.2.0.0 mask 255.255.0.0
      IP Ranges from 10.2.0.0 to 10.2.0.255

Pool name: 2
  Network: 20.1.1.0 mask 255.255.255.0
    IP ranges from 20.1.1.0 to 20.1.1.255
```

Table 4 Command output

Field	Description
Pool name	Name of the address pool.
Network	Assignable network.
IP ranges	Assignable IP address range.
Secondary networks	Assignable secondary networks.

Related commands

address range

dhcp server ip-pool

network

display dhcp server ip-in-use

Use **display dhcp server ip-in-use** to display binding information about assigned IP addresses.

Syntax

display dhcp server ip-in-use [**ip** *ip-address* | **pool** *pool-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ip *ip-address*: Displays binding information about the specified assigned IP address. If you do not specify an IP address, this command displays binding information about all assigned IP addresses.

pool *pool-name*: Displays binding information about assigned IP addresses in the specified address pool. The pool name is a case-insensitive string of 1 to 63 characters. If you do not specify an address pool, this command displays binding information about assigned IP addresses in all address pools.

Usage guidelines

The binding information can be used by other security modules only when the DHCP server is configured on the gateway of DHCP clients.

If the lease deadline exceeds the year 2100, the lease expiration time is displayed as **After 2100**.

Examples

Display binding information about all assigned DHCP addresses.

```
<Sysname> display dhcp server ip-in-use
IP address       Client-identifier/    Lease expiration      Type
                 Hardware address
10.1.1.1         4444-4444-4444        Not used              Static(F)
10.1.1.2         3030-3030-2e30-3030-  May 1 14:02:49 2015   Auto(C)
                 662e-3030-3033-2d45-
                 7468-6572-6e65-74
10.1.1.3         1111-1111-1111        After 2100            Static(C)
```

Table 5 Command output

Field	Description
IP address	IP address assigned.
Client-identifier/Hardware address	Client ID or hardware address.
Lease expiration	Lease expiration time: • **Exact time (May 1 14:02:49 2015 in this example)**—Time when the lease will expire. • **Not used**—The IP address of the static binding has not been assigned to the specific client. • **Unlimited**—Infinite lease expiration time. • **After 2100**—The lease will expire after 2100.
Type	Binding types: • **Static(F)**—A free static binding whose IP address has not been assigned. • **Static(O)**—An offered static binding whose IP address has been selected and sent by the DHCP server in a DHCP-OFFER packet to the client. **Static(C)**—A committed static binding whose IP address has been assigned to the DHCP client. • **Auto(O)**—An offered dynamic binding whose IP address has been dynamically selected by the DHCP server and sent in a DHCP-OFFER packet to the DHCP client. • **Auto(C)**—A committed dynamic binding whose IP address has been dynamically assigned to the DHCP client.

Related commands

reset dhcp server ip-in-use

display dhcp server pool

Use **display dhcp server pool** to display information about a DHCP address pool.

Syntax

display dhcp server pool [*pool-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

pool-name: Displays information about the specified address pool. The pool name is a case-insensitive string of 1 to 63 characters. If you do not specify the *pool-name* argument, this command displays information about all address pools.

Examples

Display information about all DHCP address pools.

```
<Sysname> display dhcp server pool
Pool name: 0
  Network 20.1.1.0 mask 255.255.255.0
  class a range 20.1.1.50 20.1.1.60
  bootfile-name abc.cfg
  dns-list 20.1.1.66 20.1.1.67 20.1.1.68
  domain-name www.aabbcc.com
  bims-server ip 192.168.0.51 sharekey cipher $c$3$K13OmQPi791YvQoF2Gs1E+65LOU=
  option 2 ip-address 1.1.1.1
  expired day 1 hour 2 minute 3 second 0

Pool name: 1
  Network 20.1.2.0 mask 255.255.255.0
  secondary networks:
    20.1.3.0 mask 255.255.255.0
    20.1.4.0 mask 255.255.255.0
  bims-server ip 192.168.0.51 port 50 sharekey cipher $c$3$K13OmQPi791YvQoF2Gs1E+65LOU=
  forbidden-ip 20.1.1.22 20.1.1.36 20.1.1.37
  forbidden-ip 20.1.1.22 20.1.1.23 20.1.1.24
  gateway-list 20.1.1.1 20.1.1.2 20.1.1.4
  nbns-list 20.1.1.5 20.1.1.6 20.1.1.7
  netbios-type m-node
  option 2 ip-address 1.1.1.1
  expired day 1 hour 0 minute 0 second 0

Pool name: 2
```

```
  Network 20.1.3.0 mask 255.255.255.0
  address range 20.1.3.1 to 20.1.3.15
  class departmentA range 20.1.3.20 to 20.1.3.29
  class departmentB range 20.1.3.30 to 20.1.3.40
  next-server 20.1.3.33
  tftp-server domain-name www.dian.org.cn
  tftp-server ip-address 192.168.0.120
  voice-config ncp-ip 20.1.3.2
  voice-config as-ip 20.1.3.5
  voice-config voice-vlan 3 enable
  voice-config fail-over 20.1.3.6 123*
  option 2 ip-address 20.1.3.10
  expired day 1 hour 0 minute 0 second 0

Pool name: 3
  static bindings:
    ip-address 10.10.1.2 mask 255.0.0.0
      hardware-address 00e0-00fc-0001 ethernet
    ip-address 10.10.1.3 mask 255.0.0.0
      client-identifier aaaa-bbbb
  expired unlimited
```

Table 6 Command output

Field	Description
Pool name	Name of an address pool.
Network	Assignable network.
secondary networks	Assignable secondary networks.
address range	Assignable address range.
class *class-name* range	DHCP user class and its address range.
static bindings	Static IP-to-MAC/client ID bindings.
option	Customized DHCP option.
expired	Lease duration.
bootfile-name	Boot file name
dns-list	DNS server IP address.
domain-name	Domain name suffix.
bims-server	BIMS server information.
forbidden-ip	IP addresses excluded from dynamic allocation.
gateway-list	Gateway addresses.
nbns-list	WINS server addresses.
netbios-type	NetBIOS node type.
next-server	Next server IP address.
tftp-server domain-name	TFTP server name.
tftp-server ip-address	TFTP server address.

Field	Description
voice-config ncp-ip	Primary network calling processor address.
voice-config as-ip	Backup network calling processor address.
voice-config voice-vlan	Voice VLAN.
voice-config fail-over	Failover route.

display dhcp server statistics

Use **display dhcp server statistics** to display the DHCP server statistics.

Syntax

display dhcp server statistics [**pool** *pool-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

pool *pool-name*: Specifies an address pool by its name, a case-insensitive string of 1 to 63 characters. If you do not specify this option, this command displays information about all address pools.

Examples

Display the DHCP server statistics.

```
<Sysname> display dhcp server statistics
    Pool number:                    1
    Pool utilization:               0.39%
    Bindings:
      Automatic:                    1
      Manual:                       0
      Expired:                      0
    Conflict:                       1
    Messages received:             10
      DHCPDISCOVER:                 5
      DHCPREQUEST:                  3
      DHCPDECLINE:                  0
      DHCPRELEASE:                  2
      DHCPINFORM:                   0
      BOOTPREQUEST:                 0
    Messages sent:                  6
      DHCPOFFER:                    3
      DHCPACK:                      3
      DHCPNAK:                      0
      BOOTPREPLY:                   0
    Bad Messages:                   0
```

Table 7 Command output

Field	Description
Pool number	Total number of address pools. This field is not displayed when you display statistics for a specific address pool.
Pool utilization	Pool usage rate: • If you display statistics for all address pools, this field displays the usage rate of all address pools. • If you display statistics for an address pool, this field displays the pool usage rate of the specified address pool.
Bindings	Bindings include the following types: • **Automatic**—Number of dynamic bindings. • **Manual**—Number of static bindings. • **Expired**—Number of expired bindings.
Conflict	Total number of conflict addresses. This field is not displayed if you display statistics for a specific address pool.
Messages received	DHCP packets received from clients: • DHCPDISCOVER. • DHCPREQUEST. • DHCPDECLINE. • DHCPRELEASE. • DHCPINFORM. • BOOTPREQUEST. This field is not displayed if you display statistics for a specific address pool.
Messages sent	DHCP packets sent to clients: • DHCPOFFER. • DHCPACK. • DHCPNAK. • BOOTPREPLY. This field is not displayed if statistics about a specific address pool are displayed.
Bad Messages	Number of bad messages. This field is not displayed if you display statistics for a specific address pool.

Related commands

`reset dhcp server statistics`

dns-list

Use **`dns-list`** to specify DNS server addresses in a DHCP address pool.

Use **`undo dns-list`** to remove DNS server addresses from a DHCP address pool.

Syntax

`dns-list` *`ip-address`*`&<1-8>`

`undo dns-list` [*`ip-address`*`&<1-8>`]

Default

No DNS server address is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

ip-address&<1-8>: Specifies a space-separated list of up to eight DNS servers.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

If you do not specify any parameters, the **undo dns-list** command deletes all DNS server addresses in the DHCP address pool.

Examples

Specify DNS server address 10.1.1.254 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] dns-list 10.1.1.254
```

Related commands

display dhcp server pool

domain-name

Use **domain-name** to specify a domain name in a DHCP address pool.

Use **undo domain-name** to restore the default.

Syntax

domain-name *domain-name*

undo domain-name

Default

No domain name is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

domain-name: Specifies the domain name, a case-sensitive string of 1 to 50 characters.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify domain name **company.com** in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] domain-name company.com
```

Related commands

display dhcp server pool

expired

Use **expired** to set the lease duration in a DHCP address pool.

Use **undo expired** to restore the default lease duration for a DHCP address pool.

Syntax

expired { **day** *day* [**hour** *hour* [**minute** *minute* [**second** *second*]]] | **unlimited** }

undo expired

Default

The lease duration of a dynamic DHCP address pool is one day.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

day *day*: Specifies the number of days, in the range of 0 to 365.

hour *hour*: Specifies the number of hours, in the range of 0 to 23. The default is 0.

minute *minute*: Specifies the number of minutes, in the range of 0 to 59. The default is 0.

second *second*: Specifies the number of seconds, in the range of 0 to 59. The default is 0.

unlimited: Specifies the unlimited lease duration, which is actually 136 years.

Usage guidelines

The DHCP server assigns an IP address together with the lease duration to the DHCP client. Before the lease expires, the DHCP client must extend the lease duration.

- If the lease extension operation succeeds, the DHCP client can continue to use the IP address.
- If the lease extension operation does not succeed, both of the following events occur:
  - The DHCP client cannot use the IP address after the lease duration expires.
  - The DHCP server will label the IP address as an expired address.

Examples

Set the lease duration to 1 day, 2 hours, 3 minutes, and 4 seconds in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] expired day 1 hour 2 minute 3 second 4
```

Related commands

display dhcp server expired

display dhcp server pool

reset dhcp server expired

forbidden-ip

Use **forbidden-ip** to exclude IP addresses from dynamic allocation in an address pool.

Use **undo forbidden-ip** to remove the configuration.

Syntax

forbidden-ip *ip-address*&<1-8>

undo forbidden-ip [*ip-address*&<1-8>]

Default

No IP addresses are excluded from dynamic allocation in an address pool.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

ip-address&<1-8>: Specifies a space-separated list of up to eight excluded IP addresses.

Usage guidelines

The excluded IP addresses in an address pool are still assignable in other address pools.

You can exclude a maximum of 4096 IP addresses in an address pool by executing this command multiple times.

If you do not specify any parameters, the **undo forbidden-ip** command removes all excluded IP addresses.

Examples

Exclude IP addresses 192.168.1.3 and 192.168.1.10 from dynamic allocation in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] forbidden-ip 192.168.1.3 192.168.1.10
```

Related commands

dhcp server forbidden-ip

display dhcp server pool

gateway-list

Use **gateway-list** to specify gateway addresses in a DHCP address pool or a DHCP secondary subnet.

Use **undo gateway-list** to remove the specified gateway addresses from a DHCP address pool or a DHCP secondary subnet.

Syntax

gateway-list *ip-address*&<1-64>

undo gateway-list [*ip-address*&<1-64>]

Default

No gateway address is configured in a DHCP address pool or a DHCP secondary subnet.

Views

DHCP address pool view

DHCP secondary subnet view

Predefined user roles

network-admin

Parameters

ip-address&<1-64>: Specifies a space-separated list of up to 64 gateway addresses. Gateway addresses must reside on the same subnet as the assignable IP addresses.

Usage guidelines

The DHCP server assigns gateway addresses to clients on a secondary subnet in the following ways:

- If gateways are specified in both address pool view and secondary subnet view, DHCP assigns those specified in the secondary subnet view.
- If gateways are specified in address pool view but not in secondary subnet view, DHCP assigns those specified in address pool view.

If you do not specify any parameters, the **undo gateway-list** command deletes all gateway addresses.

Examples

Specify gateway address 10.1.1.1 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] gateway-list 10.1.1.1
```

Related commands

display dhcp server pool

if-match

Use **if-match** to configure a match rule for a DHCP user class.

Use **undo if-match** to delete a match rule for a DHCP user class.

Syntax

if-match rule *rule-number* { **hardware-address** *hardware-address* **mask** *hardware-address-mask* | **option** *option-code* [**ascii** *ascii-string* [**offset** *offset* | **partial**] | **hex** *hex-string* [**mask** *mask* | **offset** *offset* **length** *length* | **partial**]] | **relay-agent** *gateway-address* }

undo if-match rule *rule-number*

Default

No match rules are configured for the DHCP user class.

Views

DHCP user class view

Predefined user roles

network-admin

Parameters

rule *rule-number*: Assigns the match rule an ID in the range of 1 to 16. A smaller ID represents a higher match priority.

hardware-address *hardware-address*: Specifies a hardware address, a string of 4 to 39 characters. The string contains hyphen-separated hexadecimal numbers. The last hexadecimal number can be a two-digit or four-digit number, and the other hexadecimal numbers must be four-digit numbers. For example, **aabb-ccdd-ee** is valid, and **aabb-c-dddd** or **aabb-cc-dddd** is invalid.

mask *hardware-address-mask*: Specifies the mask to be ANDed with the specified hardware address for the match operation. The length of the mask must be the same as that of the hardware address.

option *option-code*: Specifies a DHCP option by its number in the range of 1 to 254.

ascii *ascii-string*: Specifies an ASCII string of 1 to 128 characters.

offset *offset*: Specifies the offset in bytes after which the match operation starts. The value range is 0 to 254. If you do not specify an offset value, the match starts from the first byte of the option content. If you specify an ASCII string, a packet matches the rule if the option content after the offset is the same as the ASCII string. If you specify a hexadecimal number, a packet matches the rule if the option content of the specified length after the offset is the same as the hexadecimal number.

partial: Enables partial match. A packet matches a rule if the specified option in the packet contains the ASCII string or hexadecimal number specified in the rule. For example, if you specify **abc** in the rule, option content **xabc**, **xyzabca**, **xabcyz**, and **abcxyz** all match the rule.

hex *hex-string*: Specifies a hexadecimal number. The length of the hexadecimal number must be an even number in the range of 2 to 256.

mask *mask*: Specifies a hexadecimal mask for the match operation. The mask length must be an even number in the range of 2 to 256 and be the same as the *hex-string* length. The DHCP server selects option content of the mask length from the start and ANDs the selected option content and the specified hexadecimal number with the mask. The packet matches the rule if the two AND operation results are the same.

length *length*: Specifies the length of the option content to be matched, in the range of 1 to 128 bytes. The length must be the same as the *hex-string* length.

relay-agent *gateway-address*: Specifies a **giaddr** field value. The value is an IPv4 address in the dotted decimal notation. A packet matches the rule if its **giaddr** field value is the same as that in the rule.

Usage guidelines

If a DHCP request sent by a DHCP client matches a rule in a DHCP user class, the DHCP client matches the user class.

You can configure multiple match rules for a DHCP user class. Each match rule is uniquely identified by a rule ID within its type (hardware address, option, or relay agent address).

- If the rule that you are configuring has the same ID and type as an existing rule, the new rule overwrites the existing rule.
- If the rule that you are configuring has the same ID as an existing rule but a different type, the new rule takes effect and coexists with the existing rule. As a best practice, do not assign the same ID to rules of different types.
- Rules of different IDs cannot have the same rule content.

When you configure an **if-match hardware-address** rule, follow these guidelines:

- The hardware address type supports only the MAC address. A rule does not match clients with hardware addresses of other types.
- The specified hardware address must be of the same length as the client hardware addresses to be matched. To match MAC addresses, the specified hardware address must be six bytes long.
- The fs and 0s in the mask for the hardware match operation can be noncontiguous. For example, the rule **if-match rule** 1 **hardware-address** 0094-0000-1100 **mask** ffff-0000-ff00 matches hardware addresses in which the first two bytes are 0094 and the fifth byte is 11.

When you configure an **if-match option** rule, follow these guidelines:

- To match packets that contain an option, specify only the *option-code* argument.
- To match a hexadecimal number by AND operations, specify the **option** *option-code* **hex** *hex-string* **mask** *mask* options.
- To match a hexadecimal number directly, specify the **option** *option-code* **hex** *hex-string* [**offset** *offset* **length** *length* | **partial**] options. If you do not specify the **offset**, **length**, or **partial** parameter, a packet matches a rule if the option content starts with the hexadecimal number.
- To match an ASCII string, specify the **option** *option-code* **ascii** *ascii-string* [**offset** *offset* | **partial**] options. If you do not specify the **offset** or **partial** parameter, a packet matches a rule if the option content starts with the ASCII string.

Examples

Configure match rule **1** for DHCP user class **exam** to match DHCP requests in which the hardware address is six bytes long and begins with **0094**.

```
<Sysname> system-view
[Sysname] dhcp class exam
[Sysname-dhcp-class-exam] if-match rule 1 hardware-address 0094-0000-0101 mask
ffff-0000-0000
```

Configure match rule **2** for DHCP user class **exam** to match DHCP requests that contain Option 82.

```
<Sysname> system-view
[Sysname] dhcp class exam
[Sysname-dhcp-class-exam] if-match rule 2 option 82
```

Configure match rule **3** for DHCP user class **exam**. The rule matches DHCP requests in which the highest bit of the fourth byte in Option 82 is the hexadecimal number **1**.

```
<Sysname> system-view
[Sysname] dhcp class exam
[Sysname-dhcp-class-exam] if-match rule 3 option 82 hex 00000080 mask 00000080
```

Configure match rule **4** for DHCP user class **exam**. The rule matches DHCP requests in which the first three bytes of Option 82 are the hexadecimal number **13ae92**.

```
<Sysname> system-view
[Sysname] dhcp class exam
[Sysname-dhcp-class-exam] if-match rule 4 option 82 hex 13ae92 offset 0 length 3
```

Configure match rule **5** for DHCP user class **exam**. The rule matches DHCP requests in which the Option 82 contains the hexadecimal number **13ae**.

```
<Sysname> system-view
[Sysname] dhcp class exam
[Sysname-dhcp-class-exam] if-match rule 5 option 82 hex 13ae partial
```

Configure match rule **6** for DHCP user class **exam** to match DHCP requests in which the **giaddr** field is 10.1.1.1.

```
<Sysname> system-view
[Sysname] dhcp class exam
[Sysname-dhcp-class-exam] if-match rule 6 relay-agent 10.1.1.1
```

Related commands

dhcp class

ip-in-use threshold

Use **ip-in-use threshold** to set a threshold for the address pool usage alarming.

Use **undo ip-in-use threshold** to restore the default.

Syntax

ip-in-use threshold *threshold-value*

undo ip-in-use threshold

Default

The address pool usage threshold is 100%.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the threshold for the address pool usage percentage. The value range is 1 to 100.

Usage guidelines

If you execute this command in the same address pool view multiple times, the most recent configuration takes effect.

When the address pool usage exceeds the threshold, the system sends log messages to the information center. According to the log information, you can optimize the address pool configuration. For more information about the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Set the address pool usage threshold to 85%.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool p1
[Sysname-dhcp-pool-p1] ip-in-use threshold 85
```

nbns-list

Use **nbns-list** to specify WINS server addresses in a DHCP address pool.

Use **undo nbns-list** to remove the specified WINS server addresses.

Syntax

nbns-list *ip-address*&<1-8>

undo nbns-list [*ip-address*&<1-8>]

Default

No WINS server address is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

ip-address&<1-8>: Specifies a space-separated list of up to eight WINS server IP addresses.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

If you do not specify any parameters, the **undo nbns-list** command deletes all WINS server addresses.

Examples

Specify WINS server address 10.1.1.1 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] nbns-list 10.1.1.1
```

Related commands

display dhcp server pool

netbios-type

netbios-type

Use **netbios-type** to specify the NetBIOS node type in a DHCP address pool.

Use **undo netbios-type** to restore the default.

Syntax

netbios-type { **b-node** | **h-node** | **m-node** | **p-node** }

undo netbios-type

Default

No NetBIOS node type is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

b-node: Specifies the broadcast node. A b-node client sends the destination name in a broadcast message to get the name-to-IP mapping from a server.

h-node: Specifies the hybrid node. An h-node client unicasts the destination name to a WINS server. If it does not receive a response, the h-node client broadcasts the destination name to get the mapping from a server.

m-node: Specifies the mixed node. An m-node client broadcasts the destination name. If it does not receive a response, the m-node client unicasts the destination name to the WINS server to get the mapping.

p-node: Specifies the peer-to-peer node. A p-node client sends the destination name in a unicast message to get the mapping from the WINS server.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the NetBIOS node type as p-node in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] netbios-type p-node
```

Related commands

display dhcp server pool

nbns-list

network

Use **network** to specify the subnet for dynamic allocation in a DHCP address pool.

Use **undo network** to remove the specified subnet.

Syntax

network *network-address* [*mask-length* | **mask** *mask*] [**secondary**]

undo network *network-address* [*mask-length* | **mask** *mask*] [**secondary**]

Default

No subnet is specified in a DHCP address pool.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

network-address: Specifies the subnet for dynamic allocation. If no mask length or mask is specified, the natural mask will be used.

mask-length: Specifies the mask length in the range of 1 to 30.

mask *mask*: Specifies the mask in dotted decimal format.

secondary: Specifies the subnet as a secondary subnet. If you do not specify this keyword, this command specifies the primary subnet. If the addresses in the primary subnet are used up, the DHCP server can select addresses from a secondary subnet for clients.

Usage guidelines

You can use the **secondary** keyword to specify a secondary subnet and enter its view. In secondary subnet view, you can specify gateways by using the **gateway-list** command for DHCP clients in the secondary subnet.

You can specify only one primary subnet for a DHCP address pool. If you execute the **network** command multiple times, the most recent configuration takes effect.

You can specify up to 32 secondary subnets for a DHCP address pool.

The primary subnet and secondary subnets in a DHCP address pool must not have the same network address and mask.

If you have used the **address range** or **class** command in an address pool, you cannot specify a secondary subnet in the same address pool.

Modifying or removing the **network** configuration deletes the assigned addresses from the current address pool.

Examples

Specify primary subnet 192.168.8.0/24 and secondary subnet 192.168.10.0/24 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] network 192.168.8.0 mask 255.255.255.0
[Sysname-dhcp-pool-0] network 192.168.10.0 mask 255.255.255.0 secondary
[Sysname-dhcp-pool-0-secondary]
```

Related commands

display dhcp server pool

gateway-list

next-server

Use **next-server** to specify the IP address of a server in a DHCP address pool.

Use **undo next-server** to restore the default.

Syntax

next-server *ip-address*

undo next-server

Default

No server's IP address is specified in a DHCP address pool.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address of a server.

Usage guidelines

Upon startup, the DHCP client obtains an IP address and the specified server IP address. Then it contacts the specified server, such as a TFTP server, to get other boot information.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify a server's IP address 10.1.1.254 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] next-server 10.1.1.254
```

Related commands

display dhcp server pool

option

Use **option** to customize a DHCP option.

Use **undo option** to remove a customized DHCP option.

Syntax

option *code* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address*&<1-8> }

undo option *code*

Default

No DHCP option is customized.

Views

DHCP address pool view

DHCP option group view

Predefined user roles

network-admin

Parameters

code: Specifies the number of the customized option, in the range of 2 to 254, excluding 50 through 54, 56, 58, 59, 61, and 82.

ascii *ascii-string*: Specifies a case-sensitive ASCII string of 1 to 255 characters as the option content.

hex *hex-string*: Specifies a hexadecimal number as the option content. The length of the hexadecimal number must be an even number in the range of 2 to 256.

ip-address *ip-address*&<1-8>: Specifies a space-separated list of up to eight IP addresses as the option content.

Usage guidelines

The DHCP server fills the customized option with the specified ASCII string, hexadecimal number, or IP addresses, and sends it in a response to the client.

You can customize options for the following purposes:

- Add newly released options.
- Add options for which the vendor defines the contents, for example, Option 43.
- Add options for which the CLI does not provide a dedicated configuration command. For example, you can use the **option 4 ip-address 1.1.1.1** command to define the time server address 1.1.1.1 for DHCP clients.
- Add all option values if the actual requirement exceeds the limit for a dedicated option configuration command. For example, the **dns-list** command can specify up to eight DNS servers. To specify more than eight DNS server, you must use the **option 6** command to define all DNS servers.

DHCP options specified by dedicated commands take precedence over those specified by the **option** commands. For example, if a DNS server address is specified by both the **dns-list** command and the **option 6** command, the server uses the address specified by the **dns-list** command.

DHCP options specified in DHCP option groups take precedence over those specified in DHCP address pools.

If you execute this command multiple times with the same *code* specified, the most recent configuration takes effect.

Examples

Configure Option 7 to specify log server address 2.2.2.2 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] option 7 ip-address 2.2.2.2
```

Related commands

display dhcp server pool

reset dhcp server conflict

Use **reset dhcp server conflict** to clear IP address conflict information.

Syntax

reset dhcp server conflict [**ip** *ip-address*]

Views

User view

Predefined user roles

network-admin

Parameters

ip *ip-address*: Clears conflict information about the specified IP address. If you do not specify this option, this command clears all address conflict information.

Usage guidelines

Address conflicts occur when dynamically assigned IP addresses have been statically configured for other hosts. After you modify the address pool configuration, the conflicted addresses might become assignable. To assign these addresses, use the **reset dhcp server conflict** command to clear the conflict information first.

Examples

Clear all IP address conflict information.

```
<Sysname> reset dhcp server conflict
```

Related commands

display dhcp server conflict

reset dhcp server expired

Use **reset dhcp server expired** to clear binding information about expired IP addresses.

Syntax

reset dhcp server expired [**ip** *ip-address* | **pool** *pool-name*]

Views

User view

Predefined user roles

network-admin

Parameters

ip *ip-address*: Clears binding information about the specified expired IP address. If you do not specify an IP address, this command clears binding information about all expired IP addresses.

pool *pool-name*: Clears binding information about the expired IP addresses in the specified address pool. The pool name is a case-insensitive string of 1 to 63 characters. If you do not specify an address pool, this command clears binding information about expired IP addresses in all address pools.

Examples

Clear binding information about all expired IP addresses.

```
<Sysname> reset dhcp server expired
```

Related commands

display dhcp server expired

reset dhcp server ip-in-use

Use **reset dhcp server ip-in-use** to clear binding information about assigned IP addresses.

Syntax

reset dhcp server ip-in-use [**ip** *ip-address* | **pool** *pool-name*]

Views

User view

Predefined user roles

network-admin

Parameters

ip *ip-address*: Clears binding information about the specified assigned IP address. If you do not specify an IP address, this command clears binding information about all assigned IP addresses.

pool *pool-name*: Clears binding information about assigned IP addresses in the specified address pool. The pool name is a case-insensitive string of 1 to 63 characters. If you do not specify an address pool, this command clears binding information about assigned IP addresses in all address pools.

Usage guidelines

If you use this command to clear information about an assigned static binding, the static binding becomes a free static binding.

Examples

Clear binding information about IP address 10.110.1.1.

```
<Sysname> reset dhcp server ip-in-use ip 10.110.1.1
```

Related commands

display dhcp server ip-in-use

reset dhcp server statistics

Use **reset dhcp server statistics** to clear DHCP server statistics.

Syntax

reset dhcp server statistics

Views

User view

Predefined user roles

network-admin

Examples

Clear DHCP server statistics.

```
<Sysname> reset dhcp server statistics
```

Related commands

display dhcp server statistics

static-bind

Use **static-bind** to statically bind a client ID or MAC address to an IP address.

Use **undo static-bind** to remove a static binding.

Syntax

static-bind ip-address *ip-address* [*mask-length* | **mask** *mask*] { **client-identifier** *client-identifier* | **hardware-address** *hardware-address* [**ethernet** | **token-ring**] }

undo static-bind ip-address *ip-address*

Default

No static binding is specified in a DHCP address pool.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

ip-address *ip-address*: Specifies the IP address of the static binding. The natural mask is used if no mask length or mask is specified.

mask-length: Specifies the mask length in the range of 1 to 30.

mask *mask*: Specifies the mask, in dotted decimal format.

client-identifier *client-identifier*: Specifies the client ID of the static binding, a string of 4 to 254 characters. The string can contain only hexadecimal numbers and hyphen (-), in the format of H-H-H…. The last H can be a two-digit or four-digit hexadecimal number while the other Hs must be all four-digit hexadecimal numbers. For example, aabb-cccc-dd is correct, and aabb-c-dddd and aabb-cc-dddd are not correct.

hardware-address *hardware-address*: Specifies the client hardware address of the static binding, a string of 4 to 39 characters. The string can contain only hexadecimal numbers and hyphen

(-), in the format of H-H-H…. The last H can be a two-digit or four-digit hexadecimal number while the other Hs must be all four-digit hexadecimal numbers. For example, aabb-cccc-dd is correct, and aabb-c-dddd and aabb-cc-dddd are not correct.

ethernet: Specifies the client hardware address type as Ethernet. The default type is Ethernet.

token-ring: Specifies the client hardware address type as token ring.

Usage guidelines

The IP address of a static binding must not be an interface address of the DHCP server. Otherwise, an IP address conflict occurs, and the bound client cannot obtain the IP address.

You can specify multiple static bindings in an address pool. The total number of static bindings in all address pools cannot exceed 8192.

An IP address can be bound to only one DHCP client. To modify the binding for a DHCP client, first execute the **undo** form of the command to delete the existing binding and then create a new binding.

Examples

Bind IP address 10.1.1.1/24 to client ID **00aa-aabb** in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] static-bind ip-address 10.1.1.1 mask 255.255.255.0
client-identifier 00aa-aabb
```

Related commands

display dhcp server pool

tftp-server domain-name

Use **tftp-server domain-name** to specify a TFTP server name in a DHCP address pool.

Use **undo tftp-server domain-name** to restore the default.

Syntax

tftp-server domain-name *domain-name*

undo tftp-server domain-name

Default

No TFTP server name is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

domain-name: Specifies the TFTP server name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify TFTP server name **aaa** in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
```

```
[Sysname-dhcp-pool-0] tftp-server domain-name aaa
```

Related commands

display dhcp server pool

tftp-server ip-address

tftp-server ip-address

Use **tftp-server ip-address** to specify a TFTP server address in a DHCP address pool.

Use **undo tftp-server ip-address** to restore the default.

Syntax

tftp-server ip-address *ip-address*

undo tftp-server ip-address

Default

No TFTP server address is specified.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address of a TFTP server.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify TFTP server address 10.1.1.1 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] tftp-server ip-address 10.1.1.1
```

Related commands

display dhcp server pool

tftp-server domain-name

valid class

Use **valid class** to add DHCP user classes to the whitelist.

Use **undo valid class** to remove DHCP user classes from the whitelist.

Syntax

valid class *class-name*&<1-8>

undo valid class *class-name*&<1-8>

Default

No DHCP user class is listed on the whitelist.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

class-name&<1-8>: Specifies a space-separated list of up to eight DHCP user classes by their names, a case-insensitive string of 1 to 63 characters.

Usage guidelines

For this command to take effect, you must enable the DHCP user class whitelist.

Examples

Add DHCP user classes **test1** and **test2** to the whitelist in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] valid class test1 test2
```

Related commands

dhcp class

verify class

verify class

Use **verify class** to enable the DHCP user class whitelist.

Use **undo verify class** to disable the DHCP user class whitelist.

Syntax

verify class

undo verify class

Default

The DHCP user class whitelist is disabled.

Views

DHCP address pool view

Predefined user roles

network-admin

Usage guidelines

After you enable the DHCP user class whitelist, the DHCP server processes requests only from clients on the DHCP user class whitelist.

The DHCP user class whitelist does not take effect on clients that request static IP addresses, and the server always processes their requests.

Examples

Enable the DHCP user class whitelist in DHCP address pool 0.

```
[Sysname] system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] verify class
```

Related commands

valid class

voice-config

Use **voice-config** to configure the content for Option 184 in a DHCP address pool.

Use **undo voice-config** to remove the Option 184 content from a DHCP address pool.

Syntax

voice-config { **as-ip** *ip-address* | **fail-over** *ip-address dialer-string* | **ncp-ip** *ip-address* | **voice-vlan** *vlan-id* { **disable** | **enable** } }

undo voice-config [**as-ip** | **fail-over** | **ncp-ip** | **voice-vlan**]

Default

No Option 184 content is configured in a DHCP address pool.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

as-ip *ip-address*: Specifies the IP address of the backup network calling processor.

fail-over *ip-address dialer-string*: Specifies the failover IP address and dialer string. The *dialer-string* is a string of 1 to 39 characters. Valid characters are digits and asterisk (*).

ncp-ip *ip-address*: Specifies the IP address of the primary network calling processor.

voice-vlan *vlan-id*: Specifies the voice VLAN ID in the range of 2 to 4094.

- **disable**: Disables the specified VLAN. DHCP clients will not take this VLAN as their voice VLAN.
- **enable**: Enables the specified VLAN. DHCP clients will take this VLAN as their voice VLAN.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure Option 184 in DHCP address pool 0. The primary and backup network calling processors are at 10.1.1.1 and 10.2.2.2, respectively. The voice VLAN 3 is enabled. The failover IP address is 10.3.3.3. The dialer string is 99*.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] voice-config ncp-ip 10.1.1.1
[Sysname-dhcp-pool-0] voice-config as-ip 10.2.2.2
[Sysname-dhcp-pool-0] voice-config voice-vlan 3 enable
[Sysname-dhcp-pool-0] voice-config fail-over 10.3.3.3 99*
```

Related commands

display dhcp server pool

DHCP relay agent commands

dhcp relay check mac-address

Use **dhcp relay check mac-address** to enable MAC address check on the relay agent.

Use **undo dhcp relay check mac-address** to disable MAC address check on the relay agent.

Syntax

dhcp relay check mac-address

undo dhcp relay check mac-address

Default

The MAC address check feature is disabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

This feature enables the DHCP relay agent to compare the **chaddr** field of a received DHCP request with the source MAC address in the frame header. If they are the same, the DHCP relay agent forwards the request to the DHCP server. If they are not the same, the DHCP relay agent discards the request.

The MAC address check feature takes effect only when the **dhcp select relay** command has already been configured on the interface.

Enable the MAC address check feature only on the DHCP relay agent directly connected to the DHCP clients. A DHCP relay agent changes the source MAC address of DHCP packets before sending them.

Examples

Enable MAC address check on the DHCP relay agent.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp relay check mac-address
```

Related commands

dhcp select relay

dhcp relay check mac-address aging-time

Use **dhcp relay check mac-address aging-time** to set the aging time for MAC address check entries on the DHCP relay agent.

Use **undo dhcp relay check mac-address aging-time** to restore the default.

Syntax

dhcp relay check mac-address aging-time *time*

undo dhcp relay check mac-address aging-time

Default

The aging time is 30 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

time: Specifies the aging time for MAC address check entries, in the range of 30 to 600 seconds.

Usage guidelines

This command takes effect only after you execute the **dhcp relay check mac-address** command.

Examples

Set the aging time to 60 seconds for MAC address check entries on the DHCP relay agent.

```
<Sysname> system-view
[Sysname] dhcp relay check mac-address aging-time 60
```

dhcp relay client-information record

Use **dhcp relay client-information record** to enable recording client information in relay entries.

Use **undo dhcp relay client-information record** to disable the feature.

Syntax

dhcp relay client-information record

undo dhcp relay client-information record

Default

The DHCP relay agent does not record client information in relay entries.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Client information is recorded only when the DHCP relay agent is configured on the gateway of DHCP clients. A relay entry contains information about a client such as the client's IP and MAC addresses.

Disabling the recording of client information deletes all recorded relay entries.

Examples

Enable the recording of relay entries on the relay agent.

```
<Sysname> system-view
[Sysname] dhcp relay client-information record
```

Related commands

dhcp relay client-information refresh

dhcp relay client-information refresh enable

dhcp relay client-information refresh

Use **dhcp relay client-information refresh** to set the interval at which the DHCP relay agent refreshes relay entries.

Use **undo dhcp relay client-information refresh** to restore the default.

Syntax

dhcp relay client-information refresh [**auto** | **interval** *interval*]

undo dhcp relay client-information refresh

Default

The refresh interval is automatically calculated based on the number of relay entries.

Views

System view

Predefined user roles

network-admin

Parameters

auto: Automatically calculates the refresh interval. The more the entries, the shorter the refresh interval. The shortest interval is 50 ms.

interval *interval*: Specifies the refresh interval in the range of 1 to 120 seconds.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the refresh interval to 100 seconds.

```
<Sysname> system-view
[Sysname] dhcp relay client-information refresh interval 100
```

Related commands

dhcp relay client-information record

dhcp relay client-information refresh enable

dhcp relay client-information refresh enable

Use **dhcp relay client-information refresh enable** to enable the DHCP relay agent to periodically refresh dynamic relay entries.

Use **undo dhcp relay client-information refresh enable** to disable the DHCP relay agent to periodically refresh dynamic relay entries.

Syntax

dhcp relay client-information refresh enable

undo dhcp relay client-information refresh enable

Default

The DHCP relay agent periodically refreshes relay entries.

Views

System view

Predefined user roles

network-admin

Usage guidelines

A DHCP client unicasts a DHCP-RELEASE message to the DHCP server to release its IP address. The DHCP relay agent conveys the message to the DHCP server and does not remove the IP-to-MAC entry of the client.

With this feature, the DHCP relay agent uses a client's IP address to periodically send a DHCP-REQUEST message to the DHCP server.

- If the server returns a DHCP-ACK message or does not return any message within an interval, the DHCP relay agent performs the following operations:
  - Removes the relay entry.
  - Sends a DHCP-RELEASE message to the DHCP server to release the IP address.
- If the server returns a DHCP-NAK message, the relay agent keeps the entry.

With this feature disabled, the DHCP relay agent does not remove relay entries automatically. After a DHCP client releases its IP address, you must use the **reset dhcp relay client-information** on the relay agent to remove the corresponding relay entry.

Examples

Disable periodic refresh of relay entries.

```
<Sysname> system-view
[Sysname] undo dhcp relay client-information refresh enable
```

Related commands

dhcp relay client-information record

dhcp relay client-information refresh

reset dhcp relay client-information

dhcp relay dhcp-server timeout

Use **dhcp relay dhcp-server timeout** to set the DHCP server response timeout time for DHCP server switchover.

Use **undo dhcp relay dhcp-server timeout** to restore the default.

Syntax

dhcp relay dhcp-server timeout *time*

undo dhcp relay dhcp-server timeout

Default

The DHCP server response timeout time is 30 seconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

time: Specifies the DHCP server response timeout time in the range of 1 to 65535 seconds.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the DHCP server response timeout time to 60 seconds for DHCP server switchover on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] dhcp relay dhcp-server timeout 60
```

Related commands

dhcp relay server-address algorithm

dhcp relay gateway

Use **dhcp relay gateway** to specify the DHCP relay agent address to be inserted in DHCP requests.

Use **undo dhcp relay gateway** to restore the default.

Syntax

dhcp relay gateway *ip-address*

undo dhcp relay gateway

Default

The primary IP address of the interface is inserted in DHCP requests as the DHCP relay agent address.

Views

Interface view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the DHCP relay agent address. It must be an IP address of the interface.

Usage guidelines

The DHCP relay agent uses the specified IP address instead of the primary IP address of the relay interface as the DHCP relay agent address.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify 10.1.1.1 as the DHCP relay agent address to be inserted in DHCP requests on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] dhcp relay gateway 10.1.1.1
```

Related commands

gateway-list

dhcp relay information circuit-id

Use **dhcp relay information circuit-id** to configure the padding mode and padding format for the Circuit ID sub-option of Option 82.

Use **undo dhcp relay information circuit-id** to restore the default.

Syntax

dhcp relay information circuit-id { **bas** | **string** *circuit-id* | { **normal** | **verbose** [**node-identifier** { **mac** | **sysname** | **user-defined** *node-identifier* }] [**interface**] } [**format** { **ascii** | **hex** }] }

undo dhcp relay information circuit-id

Default

The padding mode is **normal** and the padding format is **hex**.

Views

Interface view

Predefined user roles

network-admin

Parameters

bas: Specifies the bas mode that uses the interface and VLAN information to pad the Circuit ID sub-option.

string *circuit-id*: Specifies the string mode that uses a case-sensitive string of 3 to 63 characters as the content of the Circuit ID sub-option.

normal: Specifies the normal mode, in which the padding content consists of the VLAN ID and port number.

verbose: Specifies the verbose mode. The padding content includes the node identifier, interface information, and VLAN ID. The default node identifier is the MAC address of the access node. The default interface information consists of the Ethernet type (fixed to **eth**), chassis number, slot number, sub-slot number, and interface number.

node-identifier: Specifies the access node identifier.

- **mac**: Uses the MAC address of the access node as the node identifier.
- **sysname**: Uses the device name as the node identifier. You can set the device name by using the **sysname** command in system view. The padding format for the device name is always ASCII regardless of the specified padding format. If the **sysname** keyword is specified, make sure the device name does not include any spaces. Otherwise, the DHCP relay agent fails to add or replace Option 82.
- **user-defined** *node-identifier:* Uses a case-sensitive string of 1 to 50 characters as the node identifier. The padding format for the specified character string is always ASCII regardless of the specified padding format.

interface: Uses the interface name as the interface information. The padding format for the interface name is always ASCII regardless of the specified padding format.

format: Specifies the padding format for the Circuit ID sub-option.

ascii: Specifies the ASCII padding format.

hex: Specifies the hex padding format.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

The padding format for the string mode, the normal mode, or the verbose mode varies by command configuration. Table 8 shows how the padding format is determined for different modes.

Table 8 Padding format for different modes

Keyword (mode)	If no padding format is set	If the padding format is ascii	If the padding format is hex
string *circuit-id*	The padding format is ASCII, and is not configurable.	N/A	N/A
normal	Hex.	ASCII.	Hex.
verbose	Hex for the VLAN ID. ASCII for the node identifier, Ethernet type, chassis number, slot number, sub-slot number, and interface number.	ASCII.	ASCII for the node identifier and Ethernet type. Hex for the chassis number, slot number, sub-slot number, interface number, and VLAN ID.

Examples

Specify the content mode as verbose, node identifier as the device name, and the padding format as ASCII for the Circuit ID sub-option.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp relay information enable
[Sysname-Vlan-interface10] dhcp relay information strategy replace
[Sysname-Vlan-interface10] dhcp relay information circuit-id verbose node-identifier
sysname format ascii
```

Related commands

dhcp relay information enable

dhcp relay information strategy

display dhcp relay information

dhcp relay information enable

Use **dhcp relay information enable** to enable the DHCP relay agent to support Option 82.

Use **undo dhcp relay information enable** to disable Option 82 support.

Syntax

dhcp relay information enable

undo dhcp relay information enable

Default

The DHCP relay agent does not support Option 82.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

This command enables the DHCP relay agent to add Option 82 to DHCP requests that do not contain Option 82 before forwarding the requests to the DHCP server. The content of Option 82 is determined by the **dhcp relay information circuit-id** and **dhcp relay information remote-id** commands. If the DHCP requests contain Option 82, the relay agent handles the requests according to the strategy configured with the **dhcp relay information strategy** command.

If this feature is disabled, the relay agent forwards requests that contain or do not contain Option 82 to the DHCP server.

Examples

Enable Option 82 support on the relay agent.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp relay information enable
```

Related commands

dhcp relay information circuit-id

dhcp relay information remote-id

dhcp relay information strategy

display dhcp relay information

dhcp relay information remote-id

Use **dhcp relay information remote-id** to configure the padding mode and padding format for the Remote ID sub-option of Option 82.

Use **undo dhcp relay information remote-id** to restore the default.

Syntax

dhcp relay information remote-id { **normal** [**format** { **ascii** | **hex** }] | **string** *remote-id* | **sysname** }

undo dhcp relay information remote-id

Default

The padding mode is **normal** and the padding format is **hex**.

Views

Interface view

Predefined user roles

network-admin

Parameters

normal: Specifies the normal mode in which the padding content is the MAC address of the receiving interface.

format: Specifies the padding format for the Remote ID sub-option. The default padding format is hex.

ascii: Specifies the ASCII padding format.

hex: Specifies the hex padding format.

string *remote-id*: Specifies the string mode that uses a case-sensitive string of 1 to 63 characters as the content of the Remote ID sub-option.

sysname: Specifies the sysname mode that uses the device name as the content of the Remote ID sub-option. You can set the device name by using the **sysname** command.

Usage guidelines

The padding format for the specified character string (**string**) or the device name (**sysname**) is always ASCII. The padding format for the **normal** mode is determined by the command.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the padding content for the Remote ID sub-option of Option 82 as **device001**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp relay information enable
[Sysname-Vlan-interface10] dhcp relay information strategy replace
[Sysname-Vlan-interface10] dhcp relay information remote-id string device001
```

Related commands

dhcp relay information enable

dhcp relay information strategy

display dhcp relay information

dhcp relay information strategy

Use **dhcp relay information strategy** to configure the strategy for the DHCP relay agent to handle messages containing Option 82.

Use **undo dhcp relay information strategy** to restore the default handling strategy.

Syntax

dhcp relay information strategy { **drop** | **keep** | **replace** }

undo dhcp relay information strategy

Default

The handling strategy for messages that contain Option 82 is **replace**.

Views

Interface view

Predefined user roles

network-admin

Parameters

drop: Drops DHCP messages that contain Option 82 messages.

keep: Keeps the original Option 82 intact and forwards the DHCP messages.

replace: Replaces the original Option 82 with the configured Option 82 before forwarding the DHCP messages.

Usage guidelines

This command takes effect only on DHCP requests that contain Option 82.

For DHCP requests that do not contain Option 82, the DHCP relay agent always adds Option 82 to the requests before forwarding the requests to the DHCP server.

If the handling strategy is **replace**, configure a padding mode and padding format for Option 82. If the handling strategy is **keep** or **drop**, you do not need to configure any padding mode or padding format. The settings do not take effect even if you configure them.

Examples

Specify the handling strategy for Option 82 as **keep**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp relay information enable
[Sysname-Vlan-interface10] dhcp relay information strategy keep
```

Related commands

dhcp relay information enable

display dhcp relay information

dhcp relay master-server switch-delay

Use **dhcp relay master-server switch-delay** to enable the switchback to the master DHCP server and set the switchback delay time.

Use **undo dhcp relay master-server switch-delay** to restore the default.

Syntax

dhcp relay master-server switch-delay *delay-time*

undo dhcp relay master-server switch-delay

Default

The DHCP relay agent does not switch back to the master DHCP server.

Views

Interface view

Predefined user roles

network-admin

Parameters

delay-time: Specifies the delay time in the range of 1 to 65535 minutes.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure the DHCP relay agent to switch back to the master DHCP server 3 minutes after it switches to a backup DHCP server on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] dhcp relay master-server switch-delay 3
```

Related commands

dhcp relay server-address algorithm

dhcp relay release ip

Use **dhcp relay release ip** to release a client IP address.

Syntax

dhcp relay release ip *ip-address*

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address to be released.

Usage guidelines

After you execute this command, the relay agent sends a DHCP-RELEASE packet to the DHCP server and removes the relay entry of the IP address. Upon receiving the packet, the server removes binding information about the specified IP address to release the IP address.

Examples

Release IP address 1.1.1.1.

```
<Sysname> system-view
[Sysname] dhcp relay release ip 1.1.1.1
```

dhcp relay server-address

Use **dhcp relay server-address** to specify DHCP servers on the DHCP relay agent.

Use **undo dhcp relay server-address** to remove DHCP servers.

Syntax

dhcp relay server-address *ip-address* [**class** *class-name*]

undo dhcp relay server-address [*ip-address* [**class** *class-name*]]

Default

No DHCP server is specified on the DHCP relay agent.

Views

Interface view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address of a DHCP server. The DHCP relay agent forwards DHCP packets received from DHCP clients to this DHCP server.

class *class-name*: Specifies a DHCP user class to match DHCP request packets. The class name is a case-sensitive string of 1 to 63 characters. If you do not specify this option, no DHCP user class is used to match DHCP requests.

Usage guidelines

The specified IP address of the DHCP server must not reside on the same subnet as the IP address of the DHCP relay agent interface. Otherwise, the DHCP clients might fail to obtain IP addresses.

You can specify a maximum of eight DHCP servers on an interface.

After receiving a DHCP request, the DHCP relay agent forwards the packets as follows:

- If the request matches a user class rule, the DHCP relay agent forwards the packet to DHCP servers that are configured with the user class.
- If the request does not match any user class rule, the DHCP relay agent forwards the request to DHCP servers with no user classes configured.

If you execute this command with the same user class but different values for the *ip-address* argument, you specify the same user class for different DHCP servers. If you execute the command with different user classes for the same *ip-address*, the most recent configuration takes effect.

If you do not specify an IP address, the **undo dhcp relay server-address** command removes all DHCP servers on the interface.

If the DHCP server selecting algorithm is **master-backup**, make sure both the master and backup servers have the same user class configured or have no user classes configured. Otherwise, DHCP clients cannot obtain IP addresses correctly.

Examples

Specify DHCP server address 1.1.1.1 on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp relay server-address 1.1.1.1
```

Related commands

dhcp select relay

display dhcp relay interface

dhcp relay server-address algorithm

Use **dhcp relay server-address algorithm** to specify the DHCP server selecting algorithm.

Use **undo dhcp relay server-address algorithm** to restore the default.

Syntax

dhcp relay server-address algorithm { **master-backup** | **polling** }

undo dhcp relay server-address algorithm

Default

The **polling** algorithm is used. The DHCP relay agent forwards DHCP requests to all DHCP servers at the same time.

Views

Interface view

Predefined user roles

network-admin

Parameters

master-backup: Forwards DHCP requests to the master DHCP server first. If the master server is not available or does not have assignable IP addresses, the relay agent forwards DHCP requests to backup DHCP servers in the order they are specified.

polling: Forwards DHCP requests to all DHCP servers at the same time.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify **master-backup** as the DHCP server selecting algorithm on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] dhcp relay server-address algorithm master-backup
```

Related commands

dhcp relay dhcp-server timeout

dhcp relay master-server switch-delay

dhcp relay server-address

remote-server algorithm

dhcp relay source-address

Use **dhcp relay source-address** to specify the source IP address for relayed DHCP requests.

Use **undo dhcp relay source-address** to restore the default.

Syntax

dhcp relay source-address { *ip-address* | **interface** *interface-type interface-number* }

undo dhcp relay source-address

Default

The DHCP relay agent uses the IP address of the interface that connects to the DHCP server as the source IP address for relayed DHCP requests.

Views

Interface view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the source IP address.

interface *interface-type interface-number*: Uses the IP address of an interface as the source IP address. The *interface-type interface-number* arguments specify an interface by its type and number.

Usage guidelines

This command is required if multiple relay interfaces share the same IP address or if a relay interface does not have routes to DHCP servers. You can use this command to specify the IP address of another interface, typically the loopback interface, on the DHCP relay agent as the source IP

address for DHCP requests. The relay interface inserts the source IP address in the source IP address field as well as the **giaddr** field in DHCP requests.

If multiple relay interfaces share the same IP address, you must also configure the relay interface to support Option 82. Upon receiving a DHCP request, the relay interface inserts the subnet information in sub-option 5 in Option 82. The DHCP server assigns an IP address according to sub-option 5. The DHCP relay agent looks the output interface up in the MAC address table to forward the DHCP reply.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify 1.1.1.1 as the source IP address for relayed DHCP requests on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] dhcp relay source-address 1.1.1.1
```

Related commands

dhcp select relay

dhcp smart-relay enable

Use **dhcp smart-relay enable** to enable the DHCP smart relay feature.

Use **undo dhcp smart-relay enable** to disable the DHCP smart relay feature.

Syntax

dhcp smart-relay enable

undo dhcp smart-relay enable

Default

The DHCP smart relay feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The smart relay feature allows the relay agent to use secondary IP addresses as the gateway address when the DHCP server does not reply the DHCP-OFFER message. The relay agent initially inserts its primary IP address in the **giaddr** field before forwarding a request to the DHCP server. If no DHCP-OFFER is returned after two retries, the relay agent switches to secondary IP addresses.

Without this feature, the relay agent always uses the primary IP address as the gateway address.

Examples

Enable the DHCP smart relay feature.

```
<Sysname> system-view
[Sysname] dhcp smart-relay enable
```

Related commands

dhcp select

gateway-list

dhcp-server timeout

Use **dhcp-server timeout** to set the DHCP server response timeout time for DHCP server switchover.

Use **undo dhcp-server timeout** to restore the default.

Syntax

dhcp-server timeout *time*

undo dhcp-server timeout

Default

The DHCP server response timeout time is 30 seconds.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

time: Specifies the DHCP server response timeout time in the range of 1 to 65535 seconds.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the DHCP server response timeout time to 60 seconds for DHCP server switchover in DHCP relay address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] dhcp-server timeout 60
```

Related commands

remote-server algorithm

display dhcp relay check mac-address

Use **display dhcp relay check mac-address** to display MAC address check entries on the relay agent.

Syntax

display dhcp relay check mac-address

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display MAC address check entries on the DHCP relay agent.

```
<Sysname> display dhcp relay check mac-address
```

```
Source-MAC        Interface                Aging-time
23f3-1122-adf1    Vlan2                    10
23f3-1122-2230    Vlan3                    30
```

Table 9 Command output

Field	Description
Source MAC	Source MAC address of the attacker.
Interface	Interface where the attack comes from.
Aging-time	Aging time of the MAC address check entry, in seconds.

display dhcp relay client-information

Use **display dhcp relay client-information** to display relay entries on the relay agent.

Syntax

display dhcp relay client-information [**interface** *interface-type interface-number* | **ip** *ip-address*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Displays relay entries on the specified interface. If you do not specify an interface, this command displays relay entries on all interfaces.

ip *ip-address*: Displays the relay entry for the specified IP address. If you do not specify an IP address, this command displays relay entries for all IP addresses.

Usage guidelines

The DHCP relay agent records relay entries only after you configure the **dhcp relay client-information record** command.

Examples

Display all relay entries on the relay agent.

```
<Sysname> display dhcp relay client-information
Total number of client-information items: 2
Total number of dynamic items: 1
Total number of temporary items: 1
IP address       MAC address      Type        Interface           VPN name
10.1.1.5         00e0-0000-0000   Temporary   Vlan2               N/A
```

Table 10 Command output

Field	Description
Total number of client-information items	Total number of relay entries.
Total number of dynamic items	Total number of dynamic relay entries.

Field	Description
Total number of temporary items	Total number of temporary relay entries.
IP address	IP address of the DHCP client.
MAC address	MAC address of the DHCP client.
Type	Relay entry type: • **Dynamic**—The relay agent creates a dynamic relay entry upon receiving an ACK response from the DHCP server. • **Temporary**—The relay agent creates a temporary relay entry upon receiving a REQUEST packet from a DHCP client.
Interface	Layer 3 interface connected to the DHCP client. **N/A** is displayed for relay entries without interface information.
VPN name	This field is not supported in the current software version. Name of the VPN instance to which the DHCP client belongs. If the DHCP client does not belong to any VPN, this field displays **N/A**.

Related commands

dhcp relay client-information record

reset dhcp relay client-information

display dhcp relay information

Use **display dhcp relay information** to display Option 82 configuration information for the DHCP relay agent.

Syntax

display dhcp relay information [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Displays Option 82 configuration information for the specified interface. If you do not specify an interface, this command displays Option 82 configuration information about all interfaces.

Examples

Display Option 82 configuration information for all interfaces.

```
<Sysname> display dhcp relay information
Interface: Vlan-interface100
   Status: Enable
   Strategy: Replace
   Circuit ID Pattern: Verbose
   Remote ID Pattern: Sysname
```

```
   Circuit ID format-type: Undefined
   Remote ID format-type: ASCII
   Node identifier: aabbcc
Interface: Vlan-interface200
   Status: Enable
   Strategy: Replace
   Circuit ID Pattern: User Defined
   Remote ID Pattern: User Defined
   Circuit ID format-type: ASCII
   Remote ID format-type: ASCII
   User defined:
   Circuit ID: vlan100
   Remote ID: device001
```

Table 11 Command output

Field	Description
Interface	Interface name.
Status	Option 82 states: • **Enable**—DHCP relay agent support for Option 82 is enabled. • **Disable**—DHCP relay agent support for Option 82 is disabled.
Strategy	Handling strategy for request messages containing Option 82, **Drop**, **Keep**, or **Replace**.
Circuit ID Pattern	Padding content mode of the Circuit ID sub-option, **Verbose**, **Normal**, or **User Defined**.
Remote ID Pattern	Padding content mode of the Remote ID sub-option, **Sysname**, **Normal**, or **User Defined**.
Circuit ID format-type	Padding format of the Circuit ID sub-option, **ASCII**, **Hex**, or **Undefined**.
Remote ID format-type	Padding format of the Remote ID sub-option, **ASCII**, **Hex**, or **Undefined**.
Node identifier	Access node identifier.
User defined	Content of the user-defined sub-options.
Circuit ID	User-defined content of the Circuit ID sub-option.
Remote ID	User-defined content of the Remote ID sub-option.

display dhcp relay server-address

Use **display dhcp relay server-address** to display DHCP server addresses configured on an interface.

Syntax

display dhcp relay server-address [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Displays DHCP server addresses on the specified interface. If you do not specify an interface, this command displays DHCP server addresses on all interfaces.

Examples

Display DHCP server addresses on all interfaces.

```
<Sysname> display dhcp relay server-address
Interface name      Server IP address   Public/VRF name      Class name
Vlan2               2.2.2.2             Y/--                 --
Vlan2               2.2.2.3             Y/--                 abc
```

Table 12 Command output

Field	Description
Interface name	Interface name.
Server IP address	DHCP server IP address.
Public/VRF name	This field is not supported in the current software version. Location of the DHCP server, which is determined by the configuration of the **dhcp relay server-address** command. • If neither the **public** keyword nor the **vpn-instance** *vpn-instance-name* option is specified, this field displays **--/--**. • If the **public** keyword is specified, this field displays **Y/--**. • If the **vpn-instance** *vpn-instance-name* option is specified, the VPN instance name is displayed after the slash (/), for example, **--/abc**.
Class name	Name of a DHCP user class to match DHCP requests. This field displays hyphens (**--**) if the **class** *class-name* option is not specified in the **dhcp relay server-address** command.

Related commands

dhcp relay server-address

display dhcp relay statistics

Use **display dhcp relay statistics** to display DHCP packet statistics on the DHCP relay agent.

Syntax

display dhcp relay statistics [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Displays DHCP packet statistics on the specified interface. If you do not specify an interface, this command displays all DHCP packet statistics on the DHCP relay agent.

Examples

Display all DHCP packet statistics on the DHCP relay agent.

```
<Sysname> display dhcp relay statistics
DHCP packets dropped:                  0
DHCP packets received from clients:    0
   DHCPDISCOVER:                       0
   DHCPREQUEST:                        0
   DHCPINFORM:                         0
   DHCPRELEASE:                        0
   DHCPDECLINE:                        0
   BOOTPREQUEST:                       0
DHCP packets received from servers:    0
   DHCPOFFER:                          0
   DHCPACK:                            0
   DHCPNAK:                            0
   BOOTPREPLY:                         0
DHCP packets relayed to servers:       0
   DHCPDISCOVER:                       0
   DHCPREQUEST:                        0
   DHCPINFORM:                         0
   DHCPRELEASE:                        0
   DHCPDECLINE:                        0
   BOOTPREQUEST:                       0
DHCP packets relayed to clients:       0
   DHCPOFFER:                          0
   DHCPACK:                            0
   DHCPNAK:                            0
   BOOTPREPLY:                         0
DHCP packets sent to servers:          0
   DHCPDISCOVER:                       0
   DHCPREQUEST:                        0
   DHCPINFORM:                         0
   DHCPRELEASE:                        0
   DHCPDECLINE:                        0
   BOOTPREQUEST:                       0
DHCP packets sent to clients:          0
   DHCPOFFER:                          0
   DHCPACK:                            0
   DHCPNAK:                            0
   BOOTPREPLY:                         0
```

Related commands

reset dhcp relay statistics

gateway-list

Use **gateway-list** to specify gateway addresses for DHCP clients in a DHCP address pool.

Use **undo gateway-list** to remove gateway addresses from a DHCP address pool.

Syntax

gateway-list *ip-address*&<1-64>

undo gateway-list [*ip-address*&<1-64>]

Default

No gateway address is specified in a DHCP address pool.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

ip-address&<1-64>: Specifies a space-separated list of up to 64 addresses.

Usage guidelines

DHCP clients of the same access type can be classified into different types by their locations. In this case, the relay interface typically has no IP address configured. You can use the **gateway-list** command to specify gateway addresses for clients matching the same DHCP address pool and bind the gateway addresses to the device's MAC address.

Upon receiving a DHCP DISCOVER or REQUEST from a client that matches a DHCP address pool, the relay agent processes the packet as follows:

1. Fills the **giaddr** field of the packet with the specified gateway address.
2. Forwards the packet to all DHCP servers in the matching DHCP address pool.

The DHCP servers select a DHCP address pool according to the gateway address.

Examples

Specify gateway address 10.1.1.1 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] gateway-list 10.1.1.1
```

Related commands

dhcp smart-relay enable

master-server switch-delay

Use **master-server switch-delay** to enable the switchback to the master DHCP server and set the switchback delay time.

Use **undo master-server switch-delay** to restore the default.

Syntax

master-server switch-delay *delay-time*

undo master-server switch-delay

Default

The DHCP relay agent does not switch back to the master DHCP server.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

delay-time: Specifies the delay time in the range of 1 to 65535 minutes.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure the DHCP relay agent to switch back to the master DHCP server 3 minutes after it switches to a backup DHCP server in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] master-server switch-delay 3
```

Related commands

remote-server algorithm

remote-server

Use **remote-server** to specify DHCP servers for a DHCP relay address pool.

Use **undo remote-server** to remove DHCP servers from a DHCP relay address pool.

Syntax

remote-server *ip-address*&<1-8>

undo remote-server [*ip-address*&<1-8>]

Default

No DHCP server is specified for the DHCP relay address pool.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

ip-address&<1-8>: Specifies a space-separated list of up to eight DHCP server addresses.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

If you do not specify a DHCP server address, the **undo remote-server** command removes all DHCP servers in the DHCP address pool.

Examples

Specify DHCP server 10.1.1.1 for DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] remote-server 10.1.1.1
```

remote-server algorithm

Use **remote-server algorithm** to specify the DHCP server selecting algorithm.

Use **undo remote-server algorithm** to restore the default.

Syntax

remote-server algorithm { **master-backup** | **polling** }

undo remote-server algorithm

Default

The **polling** algorithm is used. The DHCP relay agent forwards DHCP requests to all DHCP servers at the same time.

Views

DHCP address pool view

Predefined user roles

network-admin

Parameters

master-backup: Forwards DHCP requests to the master DHCP server first. If the master server is not available or does not have assignable IP addresses, the relay agent forwards DHCP requests to backup DHCP servers in the order they are specified.

polling: Forwards DHCP requests to all DHCP servers at the same time.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify **master-backup** as the DHCP server selecting algorithm in DHCP relay address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] remote-server algorithm master-backup
```

Related commands

dhcp relay server-address algorithm

dhcp-server timeout

master-server switch-delay

remote-server

reset dhcp relay client-information

Use **reset dhcp relay client-information** to clear relay entries on the DHCP relay agent.

Syntax

reset dhcp relay client-information [**interface** *interface-type interface-number* | **ip** *ip-address*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Clears relay entries on the specified interface. If you do not specify an interface, this command clears relay entries on all interfaces.

ip *ip-address*: Clears the relay entry for the specified IP address. If you do not specify an IP address, this command clears relay entries for all IP addresses.

Examples

Clear all relay entries on the DHCP relay agent.

```
<Sysname> reset dhcp relay client-information
```

Related commands

display dhcp relay client-information

reset dhcp relay statistics

Use **reset dhcp relay statistics** to clear relay agent statistics.

Syntax

reset dhcp relay statistics [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command clears all DHCP relay agent statistics.

Examples

Clear all DHCP relay agent statistics.

```
<Sysname> reset dhcp relay statistics
```

Related commands

display dhcp relay statistics

DHCP client commands

dhcp client class-id

Use **dhcp client class-id** to configure Option 60.

Use **undo dhcp client class-id** to restore the default.

NOTE:

This command is supported only in Release 6340 and later.

Syntax

dhcp client class-id { **ascii** *ascii-string* | **hex** *hex-string* }

undo dhcp client class-id

Default

Option 60 contains the vendor name and the product name.

Views

Interface view

Predefined user roles

network-admin

Parameters

ascii *ascii-string*: Specifies a case-sensitive ASCII string of 1 to 63 characters as the content in Option 60.

hex *hex-string*: Specifies a case-sensitive hexadecimal string of 4 to 64 characters as the value in Option 60.

Usage guidelines

Option 60 acts as a vendor class identifier (VCI). You can configure a DHCP client to send a request with Option 60 for the DHCP server to make class-based IP address assignment. When the DHCP server receives a request with Option 60 from a client, the server identifies the user class of the client. Then, the server assigns the client an IP address from the IP range specified for the user class.

By default, Option 60 contains the vendor name and the product name. To customize this option, use this command.

Examples

Configure FFFFFFFF as the content of Option 60 on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp client class-id hex FFFFFFFF
```

dhcp client dad enable

Use **dhcp client dad enable** to enable duplicate address detection.

Use **undo dhcp client dad enable** to disable duplicate address detection.

Syntax

dhcp client dad enable

undo dhcp client dad enable

Default

Duplicate address detection is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

DHCP client detects IP address conflict through ARP packets. An attacker can act as the IP address owner to send an ARP reply. This makes the client unable to use the IP address assigned by the server. As a best practice, disable duplicate address detection when ARP attacks exist on the network.

Examples

Disable the duplicate address.

```
<Sysname> system-view
[Sysname] undo dhcp client dad enable
```

dhcp client dscp

Use **dhcp client dscp** to set the DSCP value for DHCP packets sent by the DHCP client.

Use **undo dhcp client dscp** to restore the default.

Syntax

dhcp client dscp *dscp-value*

undo dhcp client dscp

Default

The DSCP value is 56 in DHCP packets sent by the DHCP client.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Sets the DSCP value for DHCP packets, in the range of 0 to 63.

Usage guidelines

The DSCP value of a packet specifies the priority level of the packet and affects the transmission priority of the packet. A bigger DSCP value represents a higher priority.

Examples

Set the DSCP value to 30 for DHCP packets sent by the DHCP client.

```
<Sysname> system-view
[Sysname] dhcp client dscp 30
```

dhcp client identifier

Use **dhcp client identifier** to configure a DHCP client ID for an interface.

Use **undo dhcp client identifier** to restore the default.

Syntax

dhcp client identifier { **ascii** *ascii-string* | **hex** *hex-string* | **mac** *interface-type interface-number* }

undo dhcp client identifier

Default

An interface generates the DHCP client ID based on its MAC address. If the interface has no MAC address, it uses the MAC address of the first Ethernet interface to generate its client ID.

Views

Interface view

Predefined user roles

network-admin

Parameters

ascii *ascii-string*: Specifies a case-sensitive ASCII string of 1 to 63 characters as the client ID.

hex *hex-string*: Specifies a hexadecimal number of 4 to 64 characters as the client ID.

mac *interface-type interface-number*: Uses the MAC address of the specified interface as a DHCP client ID. The *interface-type interface-number* argument specifies an interface by its type and number.

Usage guidelines

A DHCP client ID is added to the DHCP option 61. A DHCP server can specify IP addresses for clients based on the DHCP client ID. You can specify a DHCP client ID by performing one of the following operations:

- Naming an ASCII string or hexadecimal number as the client ID.
- Using the MAC address of an interface to generate a client ID.

Whichever method you use, make sure the IDs for different DHCP clients are unique.

Examples

Use a hexadecimal number of FFFFFFFF as the client ID for VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp client identifier hex FFFFFFFF
```

Related commands

display dhcp client

display dhcp client

Use **display dhcp client** to display DHCP client information.

Syntax

display dhcp client [**verbose**] [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

verbose: Displays detailed DHCP client information. If you do not specify this keyword, the command displays brief DHCP client information.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays DHCP client information on all interfaces.

Examples

Display brief DHCP client information on all interfaces.

```
<Sysname> display dhcp client
Vlan-interface10 DHCP client information:
 Current state: BOUND
 Allocated IP: 40.1.1.20 255.255.255.0
 Allocated lease: 259200 seconds, T1: 129600 seconds, T2: 226800 seconds
 DHCP server: 40.1.1.2
```

Display detailed DHCP client information on all interfaces.

```
<Sysname> display dhcp client verbose
Vlan-interface10 DHCP client information:
 Current state: BOUND
 Allocated IP: 40.1.1.20 255.255.255.0
 Allocated lease: 259200 seconds, T1: 129600 seconds, T2: 226800 seconds
 Lease from May 21 19:00:29 2012   to   May 31 19:00:29 2012
 DHCP server: 40.1.1.2
 Transaction ID: 0x1c09322d
 Default router: 40.1.1.2
 Classless static routes:
   Destination: 1.1.0.1, Mask: 255.0.0.0, NextHop: 192.168.40.16
   Destination: 10.198.122.63, Mask: 255.255.255.255, NextHop: 192.168.40.16
 DNS servers: 44.1.1.11 44.1.1.12
 Domain name: ddd.com
 Boot servers: 200.200.200.200  1.1.1.1
 ACS parameter:
   URL: http://192.168.1.1:7547/acs
   Username: bims
   Password: ******
 Client ID type: acsii(type value=00)
 Client ID value: 000c.29d3.8659-Vlan10
 Client ID (with type) hex: 0030-3030-632e-3239-
                            6433-2e38-3635-392d-
                            4574-6830-2f30-2f32
 T1 will timeout in 1 day 11 hours 58 minutes 52 seconds.
```

Table 13 Command output

Field	Description
DHCP client information	Information about the interface that acts as the DHCP client.

Field	Description
Current state	Current state of the DHCP client: • **HALT**—The client stops applying for an IP address. • **INIT**—The initialization state. • **SELECTING**—The client has sent out a DHCP-DISCOVER message in search for a DHCP server and is waiting for the response from DHCP servers. • **REQUESTING**—The client has sent out a DHCP-REQUEST message requesting for an IP address and is waiting for the response from DHCP servers. • **BOUND**—The client has received the DHCP-ACK message from a DHCP server and obtained an IP address successfully. • **RENEWING**—The T1 timer expires. • **REBOUNDING**—The T2 timer expires.
Allocated IP	IP address allocated by the DHCP server.
Allocated lease	Allocated lease time.
T1	1/2 lease time (in seconds) of the DHCP client IP address.
T2	7/8 lease time (in seconds) of the DHCP client IP address.
Lease from….to….	Start and end time of the lease.
DHCP server	DHCP server IP address that assigned the IP address.
Transaction ID	Transaction ID, a random number chosen by the client to identify an IP address allocation.
Default router	Gateway address assigned to the client.
Classless static routes	Classless static routes assigned to the client.
Static routes	Classful static routes assigned to the client.
DNS servers	DNS server address assigned to the client.
Domain name	Domain name suffix assigned to the client.
Boot servers	PXE server addresses (up to 16 addresses) specified for the DHCP client, which are obtained through Option 43.
ACS parameter	Parameters about the ACS.
URL	URL of the ACS.
Username	Username for logging in to the ACS.
Password	Password for logging in to the ACS. If a password is configured, this field displays **********. If no password is configured, this field is not displayed.
Client ID type	DHCP client ID type: • If an ASCII string is used as the client ID value, the type value is 00. • If the MAC address of a specific interface is used as the client ID value, the type value is 01. • If a hexadecimal number is used as the client ID value, the type value is the first two characters in the string.
Client ID value	Value of the DHCP client ID.
Client ID (with type) hex	DHCP client ID with the type field, a hexadecimal number.

Field	Description
T1 will timeout in 1 day 11 hours 58 minutes 52 seconds.	How long the T1 (1/2 lease time) timer will timeout.

Related commands

dhcp client identifier

ip address dhcp-alloc

ip address dhcp-alloc

Use **ip address dhcp-alloc** to configure an interface to use DHCP for IP address acquisition.

Use **undo ip address dhcp-alloc** to cancel an interface from using DHCP.

Syntax

ip address dhcp-alloc

undo ip address dhcp-alloc

Default

For the S3100V3-SI switch series, MS4320V2 switch series, MS4320 switch series, MS4200 switch series, and MS4300V2 switch series, an interface does not use DHCP for IP address acquisition.

For the S5110V2 switch series, S5110V2-SI switch series, S5130S-LI switch series, S5130S-SI switch series, S5000V3-EI switch series, S5000E-X switch series, WS5810-WiNet switch series, WS5820-WiNet switch series, and WAS6100 switch series:

- If the switch starts with initial configuration, an interface does not use DHCP for IP address acquisition.
- If the switch starts with factory defaults, VLAN-interface 1 obtains an IP address through DHCP.

For more information about initial configuration and factory defaults, see configuration file management configuration in *Fundamentals Configuration Guide*.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

When you execute the **undo ip address dhcp-alloc** command, the interface sends a DHCP-RELEASE message to release the IP address obtained through DHCP. If the interface is down, the message cannot be sent out. This situation can occur when a subinterface obtained an IP address through DHCP, and the **shutdown** command is executed on its primary interface. The subinterface will fail to send a DHCP-RELEASE message.

Examples

Configure VLAN-interface 10 to use DHCP for IP address acquisition.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ip address dhcp-alloc
```

DHCP snooping commands

DHCP snooping works between the DHCP client and the DHCP server or between the DHCP client and the relay agent. DHCP snooping does not work between the DHCP server and the DHCP relay agent.

dhcp snooping binding database filename

Use **dhcp snooping binding database filename** to configure the DHCP snooping device to back up DHCP snooping entries to a file.

Use **undo dhcp snooping binding database filename** to restore the default.

Syntax

dhcp snooping binding database filename { *filename* | **url** *url* [**username** *username* [**password** { **cipher** | **simple** } *string*]] }

undo dhcp snooping binding database filename

Default

The DHCP snooping device does not back up DHCP snooping entries.

Views

System view

Predefined user roles

network-admin

Parameters

filename: Specifies the name of a local backup file. For information about the *filename* argument, see *Fundamentals Configuration Guide*.

url *url*: Specifies the URL of a remote backup file, a case-sensitive string of 1 to 255 characters. Do not include a username or password in the URL. Supported path format type varies by server.

username *username*: Specifies the username for accessing the URL of the remote backup file, a case-sensitive string of 1 to 32 characters. Do not specify this option if a username is not required for accessing the URL.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 32 characters. Its encrypted form is a case-sensitive string of 1 to 73 characters. Do not specify this argument if a password is not required for accessing the URL of the remote backup file.

Usage guidelines

This command automatically creates the file if you specify a nonexistent file.

With this command executed, the DHCP snooping device backs up DHCP snooping entries immediately and runs auto backup. The DHCP snooping device, by default, waits 300 seconds after a DHCP snooping entry change to update the backup file. To change the waiting period, use the **dhcp snooping binding database update interval** command. If no DHCP snooping entry changes, the backup file is not updated.

As a best practice, back up the DHCP snooping entries to a remote file. If you use the local storage medium, the frequent erasing and writing might damage the medium and then cause the DHCP snooping device to malfunction.

When the file is on a remote device, follow these restrictions and guidelines to specify the URL, username, and password:

If the file is on an FTP server, enter URL in the following format: ftp://*server address:port/file path*, where the port number is optional.

If the file is on a TFTP server, enter URL in the following format: tftp://*server address:port/file path*, where the port number is optional.

- The username and password must be the same as those configured on the FTP server. If the server authenticates only the username, the password can be omitted.
- If the IP address of the server is an IPv6 address, enclose the address in a pair of brackets, for example, **ftp://[1::1]/database.dhcp**.
- You can also specify the DNS domain name for the server address field, for example, **ftp://company/database.dhcp**.

Examples

Configure the DHCP snooping device to back up DHCP snooping entries to file **database.dhcp**.

```
<Sysname> system-view
[Sysname] dhcp snooping binding database filename database.dhcp
```

Configure the DHCP snooping device to back up DHCP snooping entries to file **database.dhcp** in the working directory of the FTP server at 10.1.1.1.

```
<Sysname> system-view
[Sysname] dhcp snooping binding database filename url ftp://10.1.1.1/database.dhcp
username 1 password simple 1
```

Configure the DHCP snooping device to back up DHCP snooping entries to file **database.dhcp** in the working directory of the TFTP server at 10.1.1.1.

```
<Sysname> system-view
[Sysname] dhcp snooping binding database filename tftp://10.1.1.1/database.dhcp
```

Related commands

dhcp snooping binding database update interval

dhcp snooping binding database update interval

Use **dhcp snooping binding database update interval** to set the waiting time for the DHCP snooping device to update the backup file after a DHCP snooping entry change.

Use **undo dhcp snooping binding database update interval** to restore the default.

Syntax

dhcp snooping binding database update interval *interval*

undo dhcp snooping binding database update interval

Default

The DHCP snooping device waits 300 seconds to update the backup file after a DHCP snooping entry change. If no DHCP snooping entry changes, the backup file is not updated.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the waiting time in seconds, in the range of 60 to 864000.

Usage guidelines

When a DHCP snooping entry is learned, updated, or removed, the waiting period starts. The DHCP snooping device updates the backup file when the waiting period is reached. All changed entries during the period will be saved to the backup file.

The waiting time takes effect only after you configure the DHCP snooping entry auto backup by using the **dhcp snooping binding database filename** command.

Examples

Set the waiting time to 600 seconds for the DHCP snooping device to update the backup file.

```
<Sysname> system-view
[Sysname] dhcp snooping binding database update interval 600
```

Related commands

dhcp snooping binding database filename

dhcp snooping binding database update now

Use **dhcp snooping binding database update now** to manually save DHCP snooping entries to the backup file.

Syntax

dhcp snooping binding database update now

Views

System view

Predefined user roles

network-admin

Usage guidelines

Each time this command is executed, the DHCP snooping entries are saved to the backup file.

This command takes effect only after you configure the DHCP snooping auto backup by using the **dhcp snooping binding database filename** command.

Examples

Manually save DHCP snooping entries to the backup file.

```
<Sysname> system-view
[Sysname] dhcp snooping binding database update now
```

Related commands

dhcp snooping binding database filename

dhcp snooping binding record

Use **dhcp snooping binding record** to enable recording of client information in DHCP snooping entries.

Use **undo dhcp snooping binding record** to disable recording of client information in DHCP snooping entries.

Syntax

dhcp snooping binding record

undo dhcp snooping binding record

Default

DHCP snooping does not record client information.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

VLAN view

Predefined user roles

network-admin

Usage guidelines

This command enables DHCP snooping on the port directly connecting to the clients to record client information in DHCP snooping entries.

Examples

Enable the recording of client information in DHCP snooping entries on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp snooping binding record
```

dhcp snooping check mac-address

Use **dhcp snooping check mac-address** to enable MAC address check for DHCP snooping.

Use **undo dhcp snooping check mac-address** to disable MAC address check for DHCP snooping.

Syntax

dhcp snooping check mac-address

undo dhcp snooping check mac-address

Default

MAC address check for DHCP snooping is disabled.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

With MAC address check enabled, DHCP snooping compares the **chaddr** field of a received DHCP request with the source MAC address field in the frame header. If they are the same, DHCP snooping considers this request valid and forwards it to the DHCP server. If they are not the same, DHCP snooping discards the DHCP request.

Examples

Enable MAC address check for DHCP snooping.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] dhcp snooping check mac-address
```

dhcp snooping check request-message

Use **dhcp snooping check request-message** to enable DHCP-REQUEST check for DHCP snooping.

Use **undo dhcp snooping check request-message** to disable DHCP-REQUEST check for DHCP snooping.

Syntax

dhcp snooping check request-message

undo dhcp snooping check request-message

Default

DHCP-REQUEST check for DHCP snooping is disabled.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

DHCP-REQUEST packets include lease renewal packets, DHCP-DECLINE packets, and DHCP-RELEASE packets. This feature prevents unauthorized clients that forge DHCP-REQUEST packets from attacking the DHCP server.

With this feature enabled, DHCP snooping looks for a matching DHCP snooping entry for each received DHCP-REQUEST message.

- If a match is found, DHCP snooping compares the entry with the message. If they have consistent information, DHCP snooping considers the packet valid and forwards it to the DHCP server. If they have different information, DHCP snooping considers the message invalid and discards it.
- If no match is found, DHCP snooping forwards the message to the DHCP server.

Examples

Enable DHCP-REQUEST check for DHCP snooping.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp snooping check request-message
```

dhcp snooping deny

Use **dhcp snooping deny** to configure a port as DHCP packet blocking port.

Use **undo dhcp snooping deny** to restore the default.

Syntax

dhcp snooping deny

undo dhcp snooping deny

Default

A port does not block DHCP requests.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

CAUTION:

To avoid IP address acquisition failure, configure a port to block DHCP packets only if no DHCP clients are attached to it.

To enable a port on the snooping device to drop all incoming DHCP requests, configure that port as a DHCP packet blocking port.

Examples

Configure GigabitEthernet 1/0/1 as a DHCP packet blocking port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp snooping deny
```

dhcp snooping disable

Use **dhcp snooping disable** to disable DHCP snooping on an interface.

Use **undo dhcp snooping disable** to restore the default.

Syntax

dhcp snooping disable

undo dhcp snooping disable

Default

If you enable DHCP snooping globally or for a VLAN, DHCP snooping is enabled on all interfaces on the device or on all interfaces in the VLAN.

If you do not enable DHCP snooping globally or for a VLAN, DHCP snooping is disabled on all interfaces on the device or on all interfaces in the VLAN.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

This command allows you to narrow down the interface range where DHCP snooping takes effect. For example, to enable DHCP snooping globally except for a specific interface, you can enable DHCP snooping globally and execute this command on the target interface.

Examples

Disable DHCP snooping on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp snooping disable
```

dhcp snooping enable

Use **dhcp snooping enable** to enable DHCP snooping globally.

Use **undo dhcp snooping enable** to disable DHCP snooping globally.

Syntax

dhcp snooping enable

undo dhcp snooping enable

Default

DHCP snooping is disabled globally.

Views

System view

Predefined user roles

network-admin

Usage guidelines

After you enable DHCP snooping globally on the device, trusted ports forward responses from DHCP servers and untrusted ports discard responses. This mechanism ensures that DHCP clients obtain IP addresses from authorized DHCP servers.

When DHCP snooping is disabled globally, all ports on the device can forward responses from DHCP servers.

Examples

Enable DHCP snooping globally.

```
<Sysname> system-view
[Sysname] dhcp snooping enable
```

dhcp snooping enable vlan

Use **dhcp snooping enable vlan** to enable DHCP snooping for VLANs.

Use **undo dhcp snooping enable vlan** to disable DHCP snooping for VLANs.

Syntax

dhcp snooping enable vlan *vlan-id-list*

undo dhcp snooping enable vlan *vlan-id-list*

Default

DHCP snooping is disabled for all VLANs.

Views

System view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 VLAN items. Each VLAN item specifies a VLAN by VLAN ID or specifies a range of VLANs in the form of *vlan-id1* to *vlan-id2*.

The value range for the VLAN IDs is 1 to 4094. If you specify a VLAN range, the value for the *vlan-id2* argument must be greater than the value for the *vlan-id1* argument.

Usage guidelines

After you enable DHCP snooping for a VLAN, DHCP snooping untrusted ports in the VLAN discard incoming DHCP responses. This mechanism ensures that DHCP clients obtain IP addresses from authorized DHCP servers.

After you disable DHCP snooping for a VLAN, all interfaces in the VLAN can forward DHCP responses.

Examples

Enable DHCP snooping for VLANs 5, 10 to 20, and 32.

```
<Sysname> system-view
[Sysname] dhcp snooping enable vlan 5 10 to 20 32
```

dhcp snooping information circuit-id

Use **dhcp snooping information circuit-id** to configure the padding mode and padding format for the Circuit ID sub-option.

Use **undo dhcp snooping information circuit-id** to restore the default.

Syntax

dhcp snooping information circuit-id { **normal-extended** | [**vlan** *vlan-id*] **string** *circuit-id* | { **normal** | **verbose** [**node-identifier** { **mac** | **sysname** | **user-defined** *node-identifier* }] } [**format** { **ascii** | **hex** }] }

undo dhcp snooping information circuit-id [**vlan** *vlan-id*]

Default

The padding mode is normal and the padding format is hex.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

VLAN view

NOTE:

VLAN view is supported only in Release 6348P01 and later.

Predefined user roles

network-admin

Parameters

normal-extended: Specifies the extended normal mode. The padding content for the Circuit ID sub-option includes the VLAN ID, slot number, and interface number. This keyword is available only in Release 6328 and later.

vlan *vlan-id*: Pads the Circuit ID sub-option for packets received from the specified VLAN. If you do not specify a VLAN, the device pads the Circuit ID sub-option for packets received from the default VLAN.

string *circuit-id*: Specifies the string mode, in which the padding content for the Circuit ID sub-option is a case-sensitive string of 3 to 63 characters.

normal: Specifies the normal mode. The padding content includes the VLAN ID and interface number.

verbose: Specifies the verbose mode. The padding content includes the node identifier, interface information, and VLAN ID. The default node identifier is the MAC address of the access node. The default interface information consists of the Ethernet type (fixed to **eth**), chassis number, slot number, sub-slot number, and interface number.

node-identifier: Specifies the access node identifier.

- **mac**: Uses the MAC address of the access node as the node identifier.
- **sysname**: Uses the device name as the node identifier. You can set the device name by using the **sysname** command in system view. The padding format for the device name is always ASCII regardless of the specified padding format. If this keyword is specified, make sure the device name does not include any spaces. Otherwise, the DHCP snooping device fails to add or replace Option 82.
- **user-defined** *node-identifier*: Uses a case-sensitive string of 1 to 50 characters as the node identifier. The padding format for the specified character string is always ASCII regardless of the specified padding format.

format: Specifies the padding format for the Circuit ID sub-option.

ascii: Specifies the ASCII padding format.

hex: Specifies the hex padding format.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

The padding format for the string mode, the normal mode, or the verbose mode varies by command configuration. Table 14 shows how the padding format is determined for different modes.

Table 14 Padding format for different modes

Keyword (mode)	If no padding format is set	If the padding format is ascii	If the padding format is hex
string *circuit-id*	The padding format is always ASCII, and is not configurable.	N/A	N/A
normal	Hex.	ASCII.	Hex.
verbose	Hex for the VLAN ID. ASCII for the node identifier, Ethernet type, chassis number, slot number, sub-slot number, and interface number.	ASCII.	ASCII for the node identifier and Ethernet type. Hex for the chassis number, slot number, sub-slot number, interface number, and VLAN ID.

Examples

Configure verbose as the padding mode, device name as the node identifier, and ASCII as the padding format for the Circuit ID sub-option.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp snooping information enable
[Sysname-GigabitEthernet1/0/1] dhcp snooping information strategy replace
[Sysname-GigabitEthernet1/0/1] dhcp snooping information circuit-id verbose
node-identifier sysname format ascii
```

Related commands

dhcp snooping information enable

dhcp snooping information strategy

display dhcp snooping information

dhcp snooping information enable

Use **dhcp snooping information enable** to enable DHCP snooping to support Option 82.

Use **undo dhcp snooping information enable** to disable this feature.

Syntax

dhcp snooping information enable

undo dhcp snooping information enable

Default

DHCP snooping does not support Option 82.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

VLAN view

NOTE:

VLAN view is supported only in Release 6348P01 and later.

Predefined user roles

network-admin

Usage guidelines

This command enables DHCP snooping to add Option 82 into DHCP requests that do not contain Option 82 before forwarding the requests to the DHCP server. The content of Option 82 is determined by the **dhcp snooping information circuit-id** and **dhcp snooping information remote-id** commands. If the received DHCP request packets contain Option 82, DHCP snooping handles the packets according to the strategy configured by the **dhcp snooping information strategy** command.

Examples

Enable DHCP snooping to support Option 82.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp snooping information enable
```

Related commands

dhcp snooping information circuit-id

dhcp snooping information remote-id

dhcp snooping information strategy

dhcp snooping information remote-id

Use **dhcp snooping information remote-id** to configure the padding mode and padding format for the Remote ID sub-option.

Use **undo dhcp snooping information remote-id** to restore the default.

NOTE:

This command is supported only in Release 6343P08 and later.

Syntax

dhcp snooping information remote-id { **normal** [**format** { **ascii** | **hex** }] | [**vlan** *vlan-id*] { **string** *remote-id* | **sysname** } }

undo dhcp snooping information remote-id [**vlan** *vlan-id*]

Default

The padding mode is normal and the padding format is hex.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

VLAN view

NOTE:

VLAN view is supported only in Release 6348P01 and later.

Predefined user roles

network-admin

Parameters

vlan *vlan-id*: Pads the Remote ID sub-option for packets received from the specified VLAN. If you do not specify a VLAN, the device pads the Remote ID sub-option for packets received from the default VLAN.

string *remote-id*: Specifies the string mode that uses a case-sensitive string of 1 to 63 characters as the content of the Remote ID sub-option.

sysname: Specifies the sysname mode that uses the device name as the Remote ID sub-option. You can configure the device name by using the **sysname** command in system view.

normal: Specifies the normal mode. The padding content is the MAC address of the receiving interface.

format: Specifies the padding format for the Remote ID sub-option. The default padding format is hex.

ascii: Specifies the ASCII padding format.

hex: Specifies the hex padding format.

Usage guidelines

DHCP snooping uses ASCII to pad the specified string or device name for the Remote ID sub-option. The padding format for the normal padding mode is determined by the command configuration.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Pad the Remote ID sub-option with a character string of **device001**.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp snooping information enable
[Sysname-GigabitEthernet1/0/1] dhcp snooping information strategy replace
[Sysname-GigabitEthernet1/0/1] dhcp snooping information remote-id string device001
```

Related commands

dhcp snooping information enable

dhcp snooping information strategy

display dhcp snooping information

dhcp snooping information strategy

Use **dhcp snooping information strategy** to configure the handling strategy for Option 82 in request messages.

Use **undo dhcp snooping information strategy** to restore the default.

Syntax

dhcp snooping information strategy { **append** | **drop** | **keep** | **replace** }

undo dhcp snooping information strategy

Default

The handling strategy for Option 82 in request messages is **replace**.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

VLAN view

NOTE:

VLAN view is supported only in Release 6348P01 and later.

Predefined user roles

network-admin

Parameters

append: Processes a DHCP message as follows:

- If the DHCP message does not carry Option 82, the device forwards the message after adding the Option 82 according to the padding configuration.
- If the DHCP message carries Option 82, the device processes the message as follows:
  - Forwards the message after padding the Vendor-Specific sub-option with the content specified in the **dhcp snooping information vendor-specific** command.
  - Forwards the message without changing Option 82 if the **dhcp snooping information vendor-specific** command is not configured.

drop: Drops DHCP messages that contain Option 82.

keep: Keeps the original Option 82 intact and forwards the DHCP messages.

replace: Replaces the Option 82 with the configured Option 82 before forwarding the DHCP messages. If the DHCP messages do not carry Option 82, the device adds Option 82 according to the padding configuration before forwarding the DHCP messages.

Usage guidelines

This command takes effect only on DHCP requests that contain Option 82. For DHCP requests that do not contain Option 82, the DHCP snooping device always adds Option 82 into the requests before forwarding them to the DHCP server.

If the handling strategy is **append** or **replace**, configure a padding mode and a padding format for Option 82. If the handling strategy is **keep** or **drop**, you do not need to configure a padding mode or padding format for Option 82.

Examples

Specify the handling strategy for Option 82 in request messages as **keep**.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp snooping information enable
[Sysname-GigabitEthernet1/0/1] dhcp snooping information strategy keep
```

Related commands

dhcp snooping information circuit-id

dhcp snooping information remote-id

dhcp snooping information vendor-specific

dhcp snooping information vendor-specific

Use **dhcp snooping information vendor-specific** to configure the padding mode for the Vendor-Specific sub-option.

Use **undo dhcp snooping information vendor-specific** to restore the default.

Syntax

dhcp snooping information vendor-specific [**vlan** *vlan-id*] **bas** [**node-identifier** { **mac** | **sysname** | **user-defined** *string* }]

undo dhcp snooping information vendor-specific [**vlan** *vlan-id*]

Default

The device does not pad the Vendor-Specific sub-option.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

VLAN view

NOTE:

VLAN view is supported only in Release 6348P01 and later.

Predefined user roles

network-admin

Parameters

vlan *vlan-id*: Pads the Vendor-Specific sub-option for packets received from the specified VLAN. If you do not specify a VLAN, the device pads the Vendor-Specific sub-option for all packets received on the interface.

bas: Specifies the bas mode to pad the Vendor-Specific sub-option.

node-identifier: Specifies the access node identifier. If you do not specify this keyword, the device pads the Vendor-Specific sub-option with the bridge MAC address of the access node as the node identifier. The padding format for the Vendor-Specific sub-option is ASCII.

- **mac**: Uses the bridge MAC address of the access node as the node identifier.
- **sysname**: Uses the device name as the node identifier. You can set the device name by using the **sysname** command in system view. If the **sysname** keyword is specified, make sure the device name does not include any spaces. Otherwise, the DHCP snooping device fails to add the Vendor-Specific sub-option. If the device name contains more than 50 characters, only the first 50 characters are padded.
- **user-defined** *string*: Uses a case-sensitive string of 1 to 50 characters as the node identifier. Do not include any spaces in the string.

Usage guidelines

After you configure this command, the DHCP snooping device pads the Vendor-Specific sub-option after receiving a DHCP request. The device forwards the DHCP request without padding the Vendor-Specific sub-option if the following conditions exist:

- The **dhcp snooping information strategy append** command is configured.
- The length of Option 82 in the request reaches the upper limit.

Examples

Pad the Vendor-Specific sub-option in bas mode with the device name as the node identifier.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp snooping information enable
[Sysname-GigabitEthernet1/0/1] dhcp snooping information vendor-specific bas
node-identifier sysname
```

Related commands

dhcp snooping information enable

dhcp snooping information strategy

dhcp snooping log enable

Use **dhcp snooping log enable** to enable DHCP snooping logging.

Use **undo dhcp snooping log enable** to disable DHCP snooping logging.

Syntax

dhcp snooping log enable

undo dhcp snooping log enable

Default

DHCP snooping logging is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command enables the DHCP snooping device to generate DHCP snooping logs and send them to the information center. The information helps administrators locate and solve problems. For information about the log destination and output rule configuration in the information center, see *Network Management and Monitoring Configuration Guide*.

As a best practice, disable this feature if the log generation affects the device performance.

Examples

Enable DHCP snooping logging.

```
<Sysname> system-view
[Sysname] dhcp snooping log enable
```

dhcp snooping max-learning-num

Use **dhcp snooping max-learning-num** to set the maximum number of DHCP snooping entries that an interface can learn.

Use **undo dhcp snooping max-learning-num** to restore the default.

Syntax

dhcp snooping max-learning-num *max-number*

undo dhcp snooping max-learning-num

Default

The maximum number of DHCP snooping entries for an interface to learn is unlimited.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

max-number: Specifies the maximum number of DHCP snooping entries for an interface to learn. The value range is 1 to 4294967295.

Usage guidelines

When an interface learns the maximum number of DHCP snooping entries, the interface stops learning DHCP snooping entries. This does not affect the operating of the DHCP snooping feature.

Examples

Allow Layer 2 Ethernet interface GigabitEthernet 1/0/1 to learn a maximum of 10 DHCP snooping entries.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp snooping max-learning-num 10
```

dhcp snooping rate-limit

Use **dhcp snooping rate-limit** to enable DHCP snooping packet rate limit on an interface and set the limit value.

Use **undo dhcp snooping rate-limit** to disable DHCP snooping packet rate limit.

Syntax

dhcp snooping rate-limit *rate*

undo dhcp snooping rate-limit

Default

The DHCP snooping packet rate limit is disabled on an interface.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

rate: Specifies the maximum rate in Kbps. The value range is 64 to 512.

Usage guidelines

This command takes effect only when DHCP snooping is enabled.

With the rate limit feature, the interface discards DHCP packets that exceed the maximum rate.

The rate configured on a Layer 2 aggregate interface applies to all members of the aggregate interface. If a member interface leaves the aggregation group, it uses the rate configured in its Ethernet interface view.

The device-supported maximum rate is an integer multiple of eight. If you set the maximum rate to 67, the value 64 or 72 takes effect.

Examples

Set the maximum rate to 64 Kbps at which Layer 2 Ethernet interface GigabitEthernet 1/0/1 can receive DHCP packets.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp snooping rate-limit 64
```

dhcp snooping trust

Use **dhcp snooping trust** to configure a port as a trusted port.

Use **undo dhcp snooping trust** to restore the default state of a port.

Syntax

dhcp snooping trust

undo dhcp snooping trust

Default

After you enable DHCP snooping, all ports are untrusted.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

Specify the ports facing the DHCP server as trusted ports and specify the other ports as untrusted ports so DHCP clients can obtain valid IP addresses.

Examples

Specify Layer 2 Ethernet interface GigabitEthernet 1/0/1 as a trusted port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp snooping trust
```

Related commands

display dhcp snooping trust

dhcp snooping trust interface

Use **dhcp snooping trust interface** to configure an interface in a VLAN as a DHCP snooping trusted port.

Use **undo dhcp snooping trust interface** to configure an interface in a VLAN as a DHCP snooping untrusted port.

Syntax

dhcp snooping trust interface *interface-type interface-number*

undo dhcp snooping trust interface *interface-type interface-number*

Default

After you enable DHCP snooping for a VLAN, all interfaces in the VLAN are DHCP snooping untrusted ports.

Views

VLAN view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

In a VLAN, configure interfaces facing the DHCP server as trusted ports, and configure other interfaces as untrusted ports. The trusted ports forward response messages from the DHCP server to the clients. The untrusted ports connected to unauthorized DHCP servers discard incoming DHCP response messages.

You can execute this command multiple times in a VLAN to configure multiple trusted ports in the VLAN.

Make sure the specified interface is in the VLAN for which the **dhcp snooping enable vlan** command is configured.

Examples

Configure GigabitEthernet 1/0/1 as a trusted port in VLAN 1.

```
<Sysname> system-view
[Sysname] vlan 1
[Sysname-vlan 1] dhcp snooping trust interface gigabitethernet 1/0/1
```

Related commands

display dhcp snooping trust

display dhcp snooping binding

Use **display dhcp snooping binding** to display DHCP snooping entries.

Syntax

display dhcp snooping binding [**ip** *ip-address* [**vlan** *vlan-id*]] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ip *ip-address*: Displays the DHCP snooping entry for the specified IP address.

vlan *vlan-id*: Specifies the VLAN ID where the IP address resides.

verbose: Displays detailed DHCP snooping entry information. If you do not specify this keyword, the command displays brief DHCP snooping entry information.

Usage guidelines

If you do not specify any parameters, this command displays all DHCP snooping entries.

Examples

Display summary information about all DHCP snooping entries.

```
<Sysname> display dhcp snooping binding
 2 DHCP snooping entries found
 IP address      MAC address    Lease        VLAN  SVLAN Interface
 =============== ============== ============ ===== ===== =================
 1.1.1.7         0000-0101-0107 16907533     2     3     GE1/0/1
 1.1.1.11        0000-0101-010b 16907537     2     3     GE1/0/3
```

Display detailed information about all DHCP snooping entries.

```
<Sysname> display dhcp snooping binding verbose
 IP address: 1.1.1.7
 MAC address: 0000-0101-0107
 Lease: 16907553 seconds
 VLAN: 2
 SVLAN: 3
 Interface: GigabitEthernet1/0/1
 Parameter request list: 03 06 21

 IP address: 1.1.1.104
 MAC address: 0000-0101-010b
 Lease: 16907537 seconds
 VLAN: 2
 SVLAN: 3
 Interface: GigabitEthernet1/0/3
```

```
Parameter request list: 37 0B 01 0F 03 06 2C 2E 2F 1F 21 F9 2B
```

Table 15 Command output

Field	Description
DHCP snooping entries found	Number of DHCP snooping entries.
IP address	IP address assigned to the DHCP client.
MAC address	MAC address of the DHCP client.
Lease	Remaining lease duration in seconds.
VLAN	When both DHCP snooping and QinQ are enabled or the DHCP packet contains two VLAN tags, this field identifies the outer VLAN tag. Otherwise, it identifies the VLAN where the port connecting the DHCP client resides.
SVLAN	When both DHCP snooping and QinQ are enabled or the DHCP packet contains two VLAN tags, this field identifies the inner VLAN tag. Otherwise, it displays **N/A**.
Interface	Port connected to the DHCP client.
Parameter request list	Parameters that the DHCP client requests, in hexadecimal notation.

Related commands

dhcp snooping enable

reset dhcp snooping binding

display dhcp snooping binding database

Use **display dhcp snooping binding database** to display information about DHCP snooping entry auto backup.

Syntax

display dhcp snooping binding database

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display information about DHCP snooping entry auto backup.

```
<Sysname> display dhcp snooping binding database
File name               :   database.dhcp
Username                :
Password                :
Update interval         :   600 seconds
Latest write time       :   Feb 27 18:48:04 2012
Status                  :   Last write succeeded.
```

Table 16 Command output

Field	Description
File name	Name of the DHCP snooping entry backup file.
Username	Username for accessing the URL of the remote backup file.
Password	Password for accessing the URL of the remote backup file. This field displays ********** if a password is configured.
Update interval	Waiting time in seconds after a DHCP snooping entry change for the DHCP snooping device to update the backup file.
Latest write time	Time of the latest update.
Status	Status of the update: • **Writing**—The backup file is being updated. • **Last write succeeded**—The backup file was successfully updated. • **Last write failed**—The backup file failed to be updated.

display dhcp snooping information

Use **display dhcp snooping information** to display Option 82 configuration on the DHCP snooping device.

Syntax

display dhcp snooping information { **all** | **interface** *interface-type interface-number* }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

all: Displays Option 82 configuration on all Layer 2 Ethernet interfaces.

interface *interface-type interface-number*: Specifies an interface by its type and number.

Examples

Display Option 82 configuration on all interfaces.

```
<Sysname> display dhcp snooping information all
Interface: Bridge-Aggregation1
   Status: Disable
   Strategy: Drop
   Circuit ID:
     Padding format: User Defined
       User defined: abcd
     Format: ASCII
   Remote ID:
     Padding format: Normal
     Format: ASCII
```

```
Vendor-specific:
  Padding format: BAS
  Node identifier: MAC
VLAN 10:
  Circuit ID: abcd
  Remote ID: company
  Vendor-specific:
    Padding format: BAS
    Node identifier: User defined(abcd)
```

Table 17 Command output

Field	Description
Interface	Interface name.
Status	Option 82 status, **Enable** or **Disable**.
Strategy	Handling strategy for DHCP requests that contain Option 82, **Drop**, **Keep**, or **Replace**.
Circuit ID	Content of the Circuit ID sub-option.
Padding format	Padding format of Option 82: • For Circuit ID sub-option, the padding format can be Normal, **Normal-extented**, **User Defined**, **Verbose (sysname)**, **Verbose (MAC)**, or **Verbose (user defined)**. • For Remote ID sub-option, the padding format can be **Normal**, **Sysname**, or **User Defined**. • For Vendor-Specific sub-option, the padding format is **BAS**.
Node identifier	Access node identifier. • For the Circuit ID sub-option, this field displays the user-defined node identifier string. • For the Remote ID sub-option, this field displays the user-defined string. • For the Vendor-Specific sub-option, the node identifier can be **MAC**, **Sysname**, or **User Defined(string)**, where **string** in the brackets indicates the user-defined node identifier.
User defined	Content of the user-defined sub-option.
Format	Code type of Option 82 sub-option: • For Circuit ID sub-option, the code type can be **ASCII**, **Default**, or **Hex**. • For Remote ID sub-option, the code type can be **ASCII** or **Hex**.
Remote ID	Content of the Remote ID sub-option.
Vendor-specific	Content of the Vendor-Specific sub-option. This field is displayed only when the Vendor-Specific sub-option is configured.
VLAN	Pads Circuit ID, Remote ID, and Vendor-Specific sub-options in the DHCP packets received in the specified VLAN.

display dhcp snooping packet statistics

Use **display dhcp snooping packet statistics** to display DHCP packet statistics for DHCP snooping.

Syntax

display dhcp snooping packet statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays DHCP packet statistics for the master device.

Examples

Display DHCP packet statistics for DHCP snooping.

```
<Sysname> display dhcp snooping packet statistics
 DHCP packets received                  : 100
 DHCP packets sent                      : 200
 Invalid DHCP packets dropped           : 0
```

Related commands

reset dhcp snooping packet statistics

display dhcp snooping trust

Use **display dhcp snooping trust** to display information about trusted ports.

Syntax

display dhcp snooping trust

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display information about trusted ports.

```
<Sysname> display dhcp snooping trust
 DHCP snooping is enabled.
Interface                                Trusted  VLAN
============================             =======  ================
GE1/0/1                                  Trusted  -
GE1/0/2                                  -        100

VSI name                                Tunnel trusted
============================            ==============
a                                       Trusted

AC                                      Trusted
============================            ============
GE1/0/1 srv 1                           Trusted
```

Table 18 Command output

Field	Description
Interface	Interface name.
Trusted	For a DHCP snooping trusted port specified in the global DHCP snooping configuration, this field displays **Trusted**. For a trusted port specified in VLAN-based DHCP snooping configuration, this field displays a hyphen (**-**).
VLAN	VLAN to which the trusted port belongs. If the trusted port is specified in global DHCP snooping configuration, this field displays a hyphen (**-**).
VSI name	This field is not supported in the current software version. VSI name of the VXLAN tunnel interface. This field is available when you configure the tunnel interface assigned to the VSI as a DHCP snooping trusted interface by using the **dhcp snooping trust tunnel** command.
Tunnel trusted	This field is not supported in the current software version. Trusted tunnel interface specified in VXLAN-based DHCP snooping configuration.
AC	This field is not supported in the current software version. AC name, which is indicated by the interface name and Ethernet service instance name. This field is available when you configure the AC as the DHCP snooping trusted interface by using the **dhcp snooping trust** command in Ethernet service instance view.
Trusted	This field is not supported in the current software version. Trusted AC specified in VXLAN-based DHCP snooping configuration.

Related commands

dhcp snooping trust

dhcp snooping trust interface

reset dhcp snooping binding

Use **reset dhcp snooping binding** to clear DHCP snooping entries.

Syntax

reset dhcp snooping binding { **all** | **ip** *ip-address* [**vlan** *vlan-id*] }

Views

User view

Predefined user roles

network-admin

Parameters

all: Clears all DHCP snooping entries.

ip *ip-address*: Clears the DHCP snooping entry for the specified IP address.

vlan *vlan-id*: Clears DHCP snooping entries for the specified VLAN. If you do not specify a VLAN, this command clears DHCP snooping entries for the default VLAN.

Examples

Clear all DHCP snooping entries.

```
<Sysname> reset dhcp snooping binding all
```

Related commands

display dhcp snooping binding

reset dhcp snooping packet statistics

Use **reset dhcp snooping packet statistics** to clear DHCP packet statistics for DHCP snooping.

Syntax

reset dhcp snooping packet statistics [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears DHCP packet statistics for the master device.

Examples

Clear DHCP packet statistics for DHCP snooping.

```
<Sysname> reset dhcp snooping packet statistics
```

Related commands

display dhcp snooping packet statistics

BOOTP client commands

display bootp client

Use **display bootp client** to display information about a BOOTP client.

Syntax

display bootp client [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays BOOTP client information on all interfaces.

Examples

Display BOOTP client information on VLAN-interface 10.

```
<Sysname> display bootp client interface vlan-interface 10
Vlan-interface10 BOOTP client information:
Allocated IP: 169.254.0.2 255.255.0.0
Transaction ID: 0x3d8a7431
MAC Address: 00e0-fc0a-c3ef
```

Table 19 Command output

Field	Description
BOOTP client information	Information about the interface that acts as a BOOTP client.
Allocated IP	BOOTP client's IP address allocated by the BOOTP server.
Transaction ID	Value of the **XID** field in a BOOTP message. The BOOTP client chooses a random number for the **XID** field when sending a BOOTP request to the BOOTP server. It is used to match a response message from the BOOTP server. If the values of the **XID** field are different in the BOOTP response and request, the BOOTP client drops the BOOTP response.
Mac Address	MAC address of a BOOTP client.

Related commands

`ip address bootp-alloc`

ip address bootp-alloc

Use **`ip address bootp-alloc`** to configure an interface to use BOOTP for IP address acquisition.

Use **`undo ip address bootp-alloc`** to cancel an interface from using BOOTP.

Syntax

`ip address bootp-alloc`

`undo ip address bootp-alloc`

Default

An interface does not use BOOTP for IP address acquisition.

Views

Interface view

Predefined user roles

network-admin

Examples

Configure VLAN-interface 10 to use BOOTP for IP address acquisition.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ip address bootp-alloc
```

Related commands

`display bootp client`

Contents

DNS commands

display dns domain

Use **display dns domain** to display the domain name suffixes.

Syntax

display dns domain [**dynamic**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

dynamic: Displays the domain name suffixes dynamically obtained through DHCP or other protocols. If you do not specify this keyword, the command displays the statically configured and dynamically obtained domain name suffixes.

Examples

Display the statically configured and dynamically obtained domain name suffixes for the public network.

```
<Sysname> display dns domain
Type:
  D: Dynamic    S: Static

No.     Type    Domain suffix
1       S       com
2       D       net
```

Table 1 Command output

Field	Description
No.	Sequence number.
Type	Domain name suffix type: • **S**—A statically configured domain name suffix. • **D**—A domain name suffix dynamically obtained through DHCP or other protocols.
Domain suffix	Domain name suffixes.

Related commands

dns domain

display dns host

Use **display dns host** to display information about domain name-to-IP address mappings.

Syntax

display dns host [**ip** | **ipv6**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ip: Specifies type A queries. A type A query resolves a domain name to the mapped IPv4 address.

ipv6: Specifies type AAAA queries. A type AAAA query resolves a domain name to the mapped IPv6 address.

Usage guidelines

If you do not specify the **ip** or **ipv6** keyword, this command displays domain name-to-IP address mappings of all query types.

Examples

Display domain name-to-IP address mappings of all query types.

```
<Sysname> display dns host
Type:
  D: Dynamic    S: Static

Total number: 3
No.  Host name         Type  TTL        Query type   IP addresses
1    sample.com        D     3132       A            192.168.10.1
                                                     192.168.10.2
                                                     192.168.10.3
2    zig.sample.com    S     -          A            192.168.1.1
3    sample.net        S     -          AAAA         FE80::4904:4448
```

Table 2 Command output

Field	Description
No.	Sequence number.
Host name	Domain name.
Type	Domain name-to-IP address mapping type: • **S**—A static mapping configured by the **ip host** or **ipv6 host** command. • **D**—A mapping dynamically obtained through dynamic domain name resolution.
TTL	Time in seconds that a mapping can be stored in the cache. For a static mapping, a hyphen (-) is displayed.
Query type	Query type: A and AAAA.
IP addresses	Replied IP address: • For a type A query, the replied IP address is an IPv4 address. • For a type AAAA query, the replied IP address is an IPv6 address.

Related commands

ip host

ipv6 host

reset dns host

display dns server

Use **display dns server** to display IPv4 DNS server information.

Syntax

display dns server [**dynamic**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

dynamic: Displays IPv4 DNS server information dynamically obtained through DHCP or other protocols. If you do not specify this keyword, the command displays statically configured and dynamically obtained IPv4 DNS server information.

Examples

Display IPv4 DNS server information for the public network.

```
<Sysname> display dns server
Type:
  D: Dynamic    S: Static

No. Type  IP address
1   S     202.114.0.124
2   S     169.254.65.125
```

Table 3 Command output

Field	Description
No.	Sequence number.
Type	DNS server type: • **S**—A manually configured DNS server. • **D**—DNS server information dynamically obtained through DHCP or other protocols.
IP address	IPv4 address of the DNS server.

Related commands

dns server

display ipv6 dns server

Use **display ipv6 dns server** to display IPv6 DNS server information.

Syntax

display ipv6 dns server [**dynamic**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

dynamic: Displays IPv6 DNS server information dynamically obtained through DHCP or other protocols. If you do not specify this keyword, the command displays the statically configured and dynamically obtained IPv6 DNS server information.

Examples

Display IPv6 DNS server information for the public network.

```
<Sysname> display ipv6 dns server
Type:
  D: Dynamic    S: Static

No. Type  IPv6 address                              Outgoing Interface
1   S     2::2
```

Table 4 Command output

Field	Description
No.	Sequence number.
Type	DNS server type: • **S**—A manually configured DNS server. • **D**—DNS server information dynamically obtained through DHCP or other protocols.
IPv6 address	IPv6 address of the DNS server.
Outgoing Interface	Output interface.

Related commands

ipv6 dns server

dns domain

Use **dns domain** to configure a domain name suffix.

Use **undo dns domain** to delete the specified domain name suffix.

Syntax

dns domain *domain-name*

undo dns domain *domain-name*

Default

No domain name suffix is configured. Only the provided domain name is resolved.

Views

System view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a domain name suffix. It is a dot-separated, case-insensitive string that can include letters, digits, hyphens (-), underscores (_), and dots (.), for example, aabbcc.com. The domain name suffix can include a maximum of 253 characters, and each separated string includes no more than 63 characters.

Usage guidelines

For domain name resolution, the resolver automatically uses the suffix list to supply the missing part of an incomplete name entered by a user.

A domain name suffix applies to both IPv4 DNS and IPv6 DNS.

The system allows a maximum of 16 domain name suffixes for the public network.

Examples

Configure domain name suffix **com** for the public network.

```
<Sysname> system-view
[Sysname] dns domain com
```

Related commands

display dns domain

dns dscp

Use **dns dscp** to set the DSCP value for DNS packets sent by a DNS client or DNS proxy.

Use **undo dns dscp** to restore the default.

Syntax

dns dscp *dscp-value*

undo dns dscp

Default

The DSCP value is 0 in DNS packets sent by a DNS client or DNS proxy.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies the DSCP value in the range of 0 to 63.

Usage guidelines

The DSCP value of a packet specifies the priority level of the packet and affects the transmission priority of the packet. A bigger DSCP value represents a higher priority.

Examples

Set the DSCP value to 30 for outgoing DNS packets.

```
<Sysname> system-view
[Sysname] dns dscp 30
```

dns proxy enable

Use **dns proxy enable** to enable DNS proxy.

Use **undo dns proxy enable** to disable DNS proxy.

Syntax

dns proxy enable

undo dns proxy enable

Default

DNS proxy is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This configuration applies to both IPv4 DNS and IPv6 DNS.

Examples

Enable DNS proxy.

```
<Sysname> system-view
[Sysname] dns proxy enable
```

dns server

Use **dns server** to specify the IPv4 address of a DNS server.

Use **undo dns server** to remove the IPv4 address of a DNS server.

Syntax

dns server *ip-address*

undo dns server [*ip-address*]

Default

In versions earlier than Release 6348P01, in the factory-default settings, no DNS server IPv4 address is specified.

In Release 6348P01 and later:

- In the initial configuration, no DNS server address is specified.
- In the factory-default settings, a DNS server with IP address 114.114.114.114 is specified.

For more information about the initial configuration and factory-default settings, see configuration file management in *Fundamentals Configuration Guide*.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IPv4 address of a DNS server.

Usage guidelines

The device sends a DNS query request to the DNS servers in the order their IPv4 addresses are specified.

The system allows a maximum of six DNS server IPv4 addresses for the public network.

If you do not specify an IPv4 address, the **undo dns server** command removes all DNS server IPv4 addresses for the public network.

Examples

Specify DNS server IPv4 address 172.16.1.1.

```
<Sysname> system-view
[Sysname] dns server 172.16.1.1
```

Related commands

display dns server

dns source-interface

Use **dns source-interface** to specify the source interface for DNS packets.

Use **undo dns source-interface** to restore the default.

Syntax

dns source-interface *interface-type interface-number*

undo dns source-interface *interface-type interface-number*

Default

No source interface is specified for DNS packets. The device uses the primary IP address of the output interface of the matching route as the source IP address for a DNS request.

Views

System view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

This configuration applies to both IPv4 and IPv6.

In IPv4 DNS, the device uses the primary IPv4 address of the specified source interface as the source IP address of a DNS query. In IPv6 DNS, the device selects an IPv6 address of the specified source interface as the source IP address of a DNS query. The method of selecting the IPv6 address is defined in RFC 3484.

The system allows only one source interface for the public network. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify VLAN-interface 2 as the source interface for DNS packets on the public network.

```
<Sysname> system-view
[Sysname] dns source-interface vlan-interface 2
```

dns spoofing

Use **dns spoofing** to enable DNS spoofing and specify the IPv4 address for spoofing DNS requests.

Use **undo dns spoofing** to disable DNS spoofing.

Syntax

dns spoofing *ip-address*

undo dns spoofing *ip-address*

Default

DNS spoofing is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IPv4 address used to spoof DNS requests.

Usage guidelines

Use the **dns spoofing** command together with the **dns proxy enable** command.

DNS spoofing functions when the DNS proxy does not know the DNS server address or cannot reach the DNS server. It enables the DNS proxy to spoof DNS queries of type A by responding with the specified IPv4 address.

The system allows only one replied IPv4 address for the public network. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Enable DNS spoofing for the public network and specify IPv4 address 1.1.1.1 for spoofing DNS requests.

```
<Sysname> system-view
[Sysname] dns proxy enable
[Sysname] dns spoofing 1.1.1.1
```

Related commands

dns proxy enable

dns trust-interface

Use **dns trust-interface** to specify a DNS trusted interface.

Use **undo dns trust-interface** to remove a DNS trusted interface.

Syntax

dns trust-interface *interface-type interface-number*

undo dns trust-interface [*interface-type interface-number*]

Default

No DNS trusted interface is specified.

Views

System view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

By default, an interface obtains DNS suffix and DNS server information from DHCP. A network attacker might act as the DHCP server to assign a wrong DNS suffix and DNS server address to the device. As a result, the device fails to obtain the resolved IP address or might get the wrong IP address. With the DNS trusted interface specified, the device only uses the DNS suffix and DNS server information obtained through the trusted interface to avoid attacks.

This configuration applies to both IPv4 DNS and IPv6 DNS.

You can configure a maximum of 128 DNS trusted interfaces on the device.

If you do not specify an interface, the **undo dns trust-interface** command removes all DNS trusted interfaces and restores the default.

Examples

Specify VLAN-interface 2 as a DNS trusted interface.

```
<Sysname> system-view
[Sysname] dns trust-interface vlan-interface 2
```

ip host

Use **ip host** to create a host name-to-IPv4 address mapping.

Use **undo ip host** to remove a host name-to-IPv4 address mapping.

Syntax

ip host *host-name ip-address*

undo ip host *host-name ip-address*

Default

No host name-to-IPv4 address mappings exist.

Views

System view

Predefined user roles

network-admin

Parameters

host-name: Specifies a host name, a case-insensitive string of 1 to 253 characters. Valid characters are letters, digits, hyphens (-), underscores (_), and dots (.).

ip-address: Specifies the IPv4 address of the host.

Usage guidelines

The system allows a maximum of 1024 host name-to-IPv4 address mappings for the public network.

For the public network, each host name maps to only one IPv4 address. If you execute this command multiple times, the most recent configuration takes effect.

Do not use the **ping** command parameter **ip**, **-a**, **-c**, **-f**, **-h**, **-i**, **-m**, **-n**, **-p**, **-q**, **-r**, **-s**, **-t**, **-tos**, **-v**, or **-vpn-instance** as the host name. For more information about the **ping** command parameters, see *Network Management and Monitoring Command Reference*.

Examples

Map IPv4 address 10.110.0.1 to host name **aaa** for the public network.

```
<Sysname> system-view
[Sysname] ip host aaa 10.110.0.1
```

Related commands

display dns host

ipv6 dns dscp

Use **ipv6 dns dscp** to set the DSCP value for IPv6 DNS packets sent by an IPv6 DNS client or IPv6 DNS proxy.

Use **undo ipv6 dns dscp** to restore the default.

Syntax

ipv6 dns dscp *dscp-value*

undo ipv6 dns dscp

Default

The DSCP value is 0 in IPv6 DNS packets sent by an IPv6 DNS client or IPv6 DNS proxy.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies the DSCP value in the range of 0 to 63.

Usage guidelines

The DSCP value of a packet specifies the priority level of the packet and affects the transmission priority of the packet. A bigger DSCP value represents a higher priority.

Examples

Set the DSCP value to 30 for outgoing IPv6 DNS packets.

```
<Sysname> system-view
[Sysname] ipv6 dns dscp 30
```

ipv6 dns server

Use **ipv6 dns server** to specify the IPv6 address of a DNS server.

Use **undo ipv6 dns server** to remove the IPv6 address of a DNS server.

Syntax

ipv6 dns server *ipv6-address* [*interface-type interface-number*]

undo ipv6 dns server [*ipv6-address* [*interface-type interface-number*]]

Default

No DNS server IPv6 address is specified.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the IPv6 address of a DNS server.

interface-type interface-number: Specifies the output interface by its type and number. If you do not specify an interface, the device forwards DNS packets out of the output interface of the matching route. Specify this argument if the IPv6 address of the DNS server is a link-local address. Do not specify this argument if the IPv6 address of the DNS server is a global unicast address.

Usage guidelines

For dynamic DNS, the device sends a DNS query request to the DNS servers in the order their IPv6 addresses are specified.

The system allows a maximum of six DNS server IPv6 addresses for the public network.

If you do not specify an IPv6 address, the **undo ipv6 dns server** command removes all DNS server IPv6 addresses for the public network.

Examples

Specify DNS server IPv6 address 2002::1 for the public network.

```
<Sysname> system-view
[Sysname] ipv6 dns server 2002::1
```

Related commands

display ipv6 dns server

ipv6 dns spoofing

Use **ipv6 dns spoofing** to enable DNS spoofing and specify the IPv6 address to spoof DNS requests.

Use **undo ipv6 dns spoofing** to disable DNS spoofing.

Syntax

ipv6 dns spoofing *ipv6-address*

undo ipv6 dns spoofing *ipv6-address*

Default

DNS spoofing is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the IPv6 address used to spoof DNS requests.

Usage guidelines

Use the **ipv6 dns spoofing** command together with the **dns proxy enable** command.

DNS spoofing functions when the DNS proxy does not know the DNS server address or cannot reach the DNS server. It enables the DNS proxy to spoof DNS queries of type AAAA by responding with the specified IPv6 address.

The system allows only one replied IPv6 address for the public network. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Enable DNS spoofing for the public network and specify IPv6 address 2001::1 for spoofing DNS requests.

```
<Sysname> system-view
[Sysname] dns proxy enable
[Sysname] ipv6 dns spoofing 2001::1
```

Related commands

dns proxy enable

ipv6 host

Use **ipv6 host** to create a host name-to-IPv6 address mapping.

Use **undo ipv6 host** to remove a host name-to-IPv6 address mapping.

Syntax

ipv6 host *host-name ipv6-address*

undo ipv6 host *host-name ipv6-address*

Default

No host name-to-IPv6 address mappings exist.

Views

System view

Predefined user roles

network-admin

Parameters

host-name: Specifies a host name, a case-insensitive string of 1 to 253 characters. It can include letters, digits, hyphens (-), underscores (_), and dots (.).

ipv6-address: Specifies the IPv6 address of the host.

Usage guidelines

The system allows a maximum of 1024 host name-to-IPv6 address mappings for the public network.

For the public network, each host name maps to only one IPv6 address. If you execute this command multiple times, the most recent configuration takes effect.

Do not use the **ping ipv6** command parameter **-a**, **-c**, **-i**, **-m**, **-q**, **-s**, **-t**, **-tc**, **-v**, or **-vpn-instance** as the host name. For more information about the **ping ipv6** command parameters, see *Network Management and Monitoring Command Reference*.

Examples

Map IPv6 address 2001::1 to host name **aaa** for the public network.

```
<Sysname> system-view
[Sysname] ipv6 host aaa 2001::1
```

Related commands

ip host

reset dns host

Use **reset dns host** to clear dynamic DNS entries.

Syntax

reset dns host [**ip** | **ipv6**]

Views

User view

Predefined user roles

network-admin

Parameters

ip: Specifies type A queries. A type A query resolves a domain name to the mapped IPv4 address.

ipv6: Specifies type AAAA queries. A type AAAA query resolves a domain name to the mapped IPv6 address.

Usage guidelines

If you do not specify the **ip** or **ipv6** keyword, the **reset dns host** command clears dynamic DNS entries of all query types.

Examples

Clear dynamic DNS entries of all query types for the public network.

```
<Sysname> reset dns host
```

Related commands

display dns host

Contents

Basic IP forwarding commands

display fib

Use **display fib** to display FIB entries.

Syntax

display fib [*ip-address* [*mask* | *mask-length*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ip-address: Displays the FIB entry that matches the specified destination IP address.

mask: Specifies the mask for the IP address.

mask-length: Specifies the mask length for the IP address. The value range is 0 to 32.

Usage guidelines

If you specify an IP address without a mask or mask length, this command displays the longest matching FIB entry.

If you specify an IP address and a mask or mask length, this command displays the exactly matching FIB entry.

Examples

Display all FIB entries of the public network.

```
<Sysname> display fib

Destination count: 5 FIB entry count: 5

Flag:
  U:Usable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Relay     F:FRR

Destination/Mask   Nexthop         Flag     OutInterface/Token       Label
0.0.0.0/32         127.0.0.1       UH       InLoop0                  Null
1.1.1.0/24         192.168.126.1   USGF     M-GE0/0/0                Null
127.0.0.0/8        127.0.0.1       U        InLoop0                  Null
127.0.0.0/32       127.0.0.1       UH       InLoop0                  Null
127.0.0.1/32       127.0.0.1       UH       InLoop0                  Null
```

Display the FIB entries matching the destination IP address 10.2.1.1.

```
<Sysname> display fib 10.2.1.1

Destination count: 1 FIB entry count: 1
```

```
Flag:
  U:Usable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Relay     F:FRR

Destination/Mask   Nexthop         Flag     OutInterface/Token       Label
10.2.1.1/32        127.0.0.1       UH       InLoop0                  Null
```

Table 1 Command output

Field	Description
Destination count	Total number of destination addresses.
FIB entry count	Total number of FIB entries.
Destination/Mask	Destination address and the mask length.
Nexthop	Next hop address.
Flag	Flags of routes: • **U**—Usable route. • **G**—Gateway route. • **H**—Host route. • **B**—Blackhole route. • **D**—Dynamic route. • **S**—Static route. • **R**—Relay route. • **F**—Fast reroute.
OutInterface/Token	Output interface/LSP index number.
Label	Inner label.

ip forwarding-table save

Use **ip forwarding-table save** to save the IP forwarding entries to a file.

Syntax

ip forwarding-table save filename *filename*

Views

Any view

Predefined user roles

network-admin

Parameters

filename *filename*: Specifies the name of a file, a string of 1 to 255 characters. For information about the *filename* argument, see file system management in *Fundamentals Configuration Guide*.

Usage guidelines

The command automatically creates the file if you specify a nonexistent file. If the file already exists, this command overwrites the file content.

To automatically save the IP forwarding entries periodically, configure a schedule for the device to automatically run the **ip forwarding-table save** command. For information about scheduling a task, see *Fundamentals Configuration Guide*.

Examples

Save the IP forwarding entries to the **fib.txt** file.

```
<Sysname> ip forwarding-table save filename fib.txt
```

Contents

Fast forwarding commands

display ip fast-forwarding aging-time

Use **display ip fast-forwarding aging-time** to display the aging time of fast forwarding entries.

Syntax

display ip fast-forwarding aging-time

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the aging time of fast forwarding entries.

```
<Sysname> display ip fast-forwarding aging-time
 Aging time: 30s
```

Related commands

ip fast-forwarding aging-time

display ip fast-forwarding cache

Use **display ip fast-forwarding cache** to display fast forwarding entries.

Syntax

display ip fast-forwarding cache [*ip-address*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ip-address: Specifies an IP address. If you do not specify an IP address, this command displays all fast forwarding entries.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays fast forwarding entries for all member devices.

Examples

Display all fast forwarding entries.

```
<Sysname> display ip fast-forwarding cache
Total number of fast-forwarding entries: 1
SIP            SPort DIP            DPort Pro Input_If   Output_If   Flg
7.0.0.13       68    8.0.0.1        67    17  GE1/0/3    GE1/0/1     5
```

Table 1 Command output

Field	Description
SIP	Source IP address.
SPort	Source port number.
DIP	Destination IP address.
DPort	Destination port number.
Pro	Protocol number.
Input_If	Input interface type and number. If no interface is involved in fast forwarding, this field displays **N/A**. If the input interface does not exist, this field displays a hyphen (-).
Output_If	Output interface type and number. If no interface is involved in fast forwarding, this field displays **N/A**. If the output interface does not exist, this field displays a hyphen (-).
Flg	Internal tag, marking internal operation information, such as fragmentation.

Related commands

`reset ip fast-forwarding cache`

display ip fast-forwarding fragcache

Use **`display ip fast-forwarding fragcache`** to display fast forwarding entries for fragmented packets.

Syntax

`display ip fast-forwarding fragcache` [*`ip-address`*] [**`slot`** *`slot-number`*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

`ip-address`: Specifies an IP address. If you do not specify an IP address, this command displays fast forwarding entries for all fragmented packets.

`slot` *`slot-number`*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays fast forwarding entries for fragmented packets on all member devices.

Examples

Display fast forwarding entries about all fragmented packets.

```
<Sysname> display ip fast-forwarding fragcache
Total number of fragment fast-forwarding entries: 1
SIP             SPort DIP             DPort Pro Input_If    ID
```

```
7.0.0.13        68    8.0.0.1         67    17  GE1/0/3     2
```

Table 2 Command output

Field	Description
SIP	Source IP address.
SPort	Source port number.
DIP	Destination IP address.
DPort	Destination port number.
Pro	Protocol number.
Input_If	Input interface type and number. If no interface is involved in fast forwarding, this field displays **N/A**. If the input interface does not exist, this field displays a hyphen (-).
ID	Fragment ID.

Related commands

`reset ip fast-forwarding cache`

ip fast-forwarding aging-time

Use **`ip fast-forwarding aging-time`** to configure the aging time for fast forwarding entries.

Use **`undo ip fast-forwarding aging-time`** to restore the default.

Syntax

`ip fast-forwarding aging-time` *`aging-time`*

`undo ip fast-forwarding aging-time`

Default

The aging time is 30 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

`aging-time`: Specifies the aging time in the range of 10 to 300 seconds.

Examples

Set the aging time to 20 seconds for fast forwarding entries.

```
<Sysname> system-view
[Sysname] ip fast-forwarding aging-time 20
```

Related commands

`display ip fast-forwarding aging-time`

ip fast-forwarding load-sharing

Use **ip fast-forwarding load-sharing** to enable fast forwarding load sharing.

Use **undo ip fast-forwarding load-sharing** to disable fast forwarding load sharing.

Syntax

ip fast-forwarding load-sharing

undo ip fast-forwarding load-sharing

Default

Fast forwarding load sharing is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Fast forwarding load sharing enables the device to load share packets of the same flow. This feature identifies a data flow by using the packet information.

If fast forwarding load sharing is disabled, the device identifies a data flow by the packet information and the input interface. No load sharing is implemented.

Examples

Enable fast forwarding load sharing.

```
<Sysname> system-Views
[Sysname] ip fast-forwarding load-sharing
```

reset ip fast-forwarding cache

Use **reset ip fast-forwarding cache** to clear the fast forwarding table.

Syntax

reset ip fast-forwarding cache [**slot** *slot-number*]

Views

User view

Predefined use roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears the fast forwarding table for all member devices.

Examples

Clear the fast forwarding table.

```
<Sysname> reset ip fast-forwarding cache
```

Related commands

display ip fast-forwarding cache

display ip fast-forwarding fragcache

Contents

IP performance optimization commands

display icmp statistics

Use **display icmp statistics** to display ICMP statistics.

Syntax

display icmp statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays ICMP statistics for all member devices.

Usage guidelines

ICMP statistics include information about received and sent ICMP packets.

Examples

Display ICMP statistics.

```
<Sysname> display icmp statistics
  Input: bad formats   0                   bad checksum            0
         echo          175                 destination unreachable 0
         source quench 0                   redirects               0
         echo replies  201                 parameter problem       0
         timestamp     0                   information requests    0
         mask requests 0                   mask replies            0
         time exceeded 0                   invalid type            0
         router advert 0                   router solicit          0
         broadcast/multicast echo requests ignored            0
         broadcast/multicast timestamp requests ignored       0
 Output: echo          0                   destination unreachable 0
         source quench 0                   redirects               0
         echo replies  175                 parameter problem       0
         timestamp     0                   information replies     0
         mask requests 0                   mask replies            0
         time exceeded 0                   bad address             0
         packet error  1442                router advert           3
```

display ip statistics

Use **display ip statistics** to display IP packet statistics.

Syntax

display ip statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IP packet statistics for all member devices.

Usage guidelines

IP statistics include information about received and sent packets, fragments, and reassembly.

Examples

Display IP packet statistics.

```
<Sysname> display ip statistics
  Input:   sum            7120            local            112
           bad protocol   0               bad format       0
           bad checksum   0               bad options      0
  Output:  forwarding     0               local            27
           dropped        0               no route         2
           compress fails 0
  Fragment:input          0               output           0
           dropped        0
           fragmented     0               couldn't fragment 0
  Reassembling:sum        0               timeouts         0
```

Table 1 Command output

Field	Description
Input	Statistics about received packets: • **sum**—Total number of packets received. • **local**—Total number of packets destined for the device. • **bad protocol**—Total number of unknown protocol packets. • **bad format**—Total number of packets with incorrect format. • **bad checksum**—Total number of packets with incorrect checksum. • **bad options**—Total number of packets with incorrect option.
Output	Statistics about sent packets: • **forwarding**—Total number of packets forwarded. • **local**—Total number of packets locally sent. • **dropped**—Total number of packets discarded. • **no route**—Total number of packets for which no route is available. • **compress fails**—Total number of packets failed to be compressed.

Field	Description
Fragment	Statistics about fragments: • **input**—Total number of fragments received. • **output**—Total number of fragments sent. • **dropped**—Total number of fragments dropped. • **fragmented**—Total number of packets successfully fragmented. • **couldn't fragment**—Total number of packets failed to be fragmented.
Reassembling	Statistics about reassembly: • **sum**—Total number of packets reassembled. • **timeouts**—Total number of reassembly timeouts.

Related commands

display ip interface

reset ip statistics

display rawip

Use **display rawip** to display brief information about RawIP connections.

Syntax

display rawip [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays brief information about RawIP connections for all member devices.

Usage guidelines

Brief RawIP connection information includes local and peer addresses, protocol, and PCB.

Examples

Display brief information about RawIP connections.

```
<Sysname> display rawip
 Local Addr       Foreign Addr     Protocol  Slot   PCB
 0.0.0.0          0.0.0.0          1         1      0x0000000000000009
 0.0.0.0          0.0.0.0          1         1      0x0000000000000008
```

Table 2 Command output

Field	Description
Local Addr	Local IP address.
Foreign Addr	Peer IP address.
Protocol	Protocol number.

Field	Description
PCB	Protocol control block.

display rawip verbose

Use **display rawip verbose** to display detailed information about RawIP connections.

Syntax

display rawip verbose [**slot** *slot-number* [**pcb** *pcb-index*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

pcb *pcb-index*: Displays detailed RawIP connection information for the specified PCB. The *pcb-index* argument specifies the index of the PCB. The index is a hexadecimal string in the range of 1 to ffffffffffffffff.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays detailed information about RawIP connections for all member devices.

Usage guidelines

The detailed information includes socket creator, state, option, type, protocol number, and the source and destination IP addresses of RawIP connections.

Examples

Display detailed information about RawIP connections.

```
<Sysname> display rawip verbose
Total RawIP socket number: 1

 Connection info: src = 0.0.0.0, dst = 0.0.0.0
 Location: slot 6 cpu 0
 Creator: ping[320]
 State: N/A
 Options: N/A
 Error: 0
 Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 9216 / 1 / 0 / N/A
 Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A
 Type: 3
 Protocol: 1
 Inpcb flags: N/A
 Inpcb extflag: INP_EXTRCVICMPERR INP_EXTFILTER
 Inpcb vflag: INP_IPV4
 TTL: 255(minimum TTL: 0)
 Send VRF: 0xffff
 Receive VRF: 0xffff
```

Table 3 Command output

Field	Description
Total RawIP socket number	Total number of RawIP sockets.
Connection info	Connection information, including source IP address and destination IP address.
Location	Socket location. This field is not available on the centralized devices.
Creator	Name of the operation that created the socket. The number in brackets is the process number of the creator.
State	State of the socket.
Options	Socket options.
Error	Error code.

Receiving buffer (cc/hiwat/lowat/drop/state)	Displays receive buffer information in the following order:
	• **cc**—Used space.
	• **hiwat**—Maximum space.
	• **lowat**—Minimum space.
	• **drop**—Number of dropped packets.
	• **state**—Buffer state:
	  ○ **CANTSENDMORE**—Unable to send data to the peer.
	  ○ **CANTRCVMORE**—Unable to receive data from the peer.
	  ○ **RCVATMARK**—Receiving tag.
	  ○ **N/A**—None of the above states.

Sending buffer (cc/hiwat/lowat/state)	Displays send buffer information in the following order:
	• **cc**—Used space.
	• **hiwat**—Maximum space.
	• **lowat**—Minimum space.
	• **state**—Buffer state:
	  ○ **CANTSENDMORE**—Unable to send data to the peer.
	  ○ **CANTRCVMORE**—Unable to receive data from the peer.
	  ○ **RCVATMARK**—Receiving tag.
	  ○ **N/A**—None of the above states.

Type	Socket type: • **1**—**SOCK_STREAM**. This socket uses TCP to provide reliable transmission of byte streams. • **2**—**SOCK_DGRAM**. This socket uses UDP to provide datagram transmission. • **3**—**SOCK_RAW**. This socket allows an application to change the next upper-layer protocol header. • **N/A**—None of the above types.
Protocol	Number of the protocol using the socket.

Field	Description
Inpcb flags	Flags in the Internet PCB: • **INP_RECVOPTS**—Receives IP options. • **INP_RECVRETOPTS**—Receives replied IP options. • **INP_RECVDSTADDR**—Receives destination IP address. • **INP_HDRINCL**—Provides the entire IP header. • **INP_REUSEADDR**—Reuses the IP address. • **INP_REUSEPORT**—Reuses the port number. • **INP_ANONPORT**—Port number not specified. • I**NP_RECVIF**—Records the input interface of the packet. • **INP_RECVTTL**—Receives TTL of the packet. Only UDP and RawIP support this flag. • **INP_DONTFRAG**—Sets the **Don't Fragment** flag. • **INP_ROUTER_ALERT**—Receives packets with the router alert option. Only RawIP supports this flag. • **INP_PROTOCOL_PACKET**—Identifies a protocol packet. • **INP_RCVVLANID**—Receives the VLAN ID of the packet. Only UDP and RawIP support this flag. • **INP_RCVMACADDR**—Receives the MAC address of the frame. • **INP_RECVTOS**—Receives TOS of the packet. Only UDP and RawIP support this flag. • **INP_USEICMPSRC**—Uses the specified IP address as the source IP address for outgoing ICMP packets. • **INP_SYNCPCB**—Waits until Internet PCB is synchronized. • **N/A**—None of the above flags.
Inpcb extflag	Extension flags in the Internet PCB: • **INP_EXTRCVPVCIDX**—Records the PVC index of the received packet. • **INP_RCVPWID**—Records the PW ID of the received packet. • **INP_EXTRCVICMPERR**—Receives an ICMP error packet. • **INP_EXTFILTER**—Filters the contents in the received packet. • **N/A**—None of the above flags.
Inpcb vflag	IP version flags in the Internet PCB: • **INP_IPV4**—IPv4 protocol. • **INP_TIMEWAIT**—In **TIMEWAIT** state. • **INP_ONESBCAST**—Sends broadcast packets. • **INP_DROPPED**—Protocol dropped flag. • **INP_SOCKREF**—Strong socket reference. • **INP_DONTBLOCK**—Do not block synchronization of the Internet PCB. • **N/A**—None of the above flags.
TTL	TTL value in the Internet PCB.
Send VRF	This field is not supported in the current software version. VRF from which packets are sent.
Receive VRF	This field is not supported in the current software version. VRF from which packets are received.

display tcp

Use **display tcp** to display brief information about TCP connections.

Syntax

display tcp [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays brief information about TCP connections for all member devices.

Usage guidelines

Brief TCP connection information includes local IP address, local port number, peer IP address, peer port number, and TCP connection state.

Examples

Display brief information about TCP connections.

```
<Sysname> display tcp
 *: TCP connection with authentication
 Local Addr:port       Foreign Addr:port     State       Slot  PCB
*0.0.0.0:21            0.0.0.0:0             LISTEN      1     0x000000000000c387
 192.168.20.200:23     192.168.20.14:1284    ESTABLISHED 1     0x0000000000000009
 192.168.20.200:23     192.168.20.14:1283    ESTABLISHED 1     0x0000000000000002
```

Table 4 Command output

Field	Description
*	Indicates that the TCP connection uses authentication.
Local Addr:port	Local IP address and port number.
Foreign Addr:port	Peer IP address and port number.
State	TCP connection state.
PCB	PCB index.

display tcp statistics

Use **display tcp statistics** to display TCP traffic statistics.

Syntax

display tcp statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays TCP traffic statistics for all member devices.

Usage guidelines

TCP traffic statistics include information about received and sent TCP packets and Syncache/syncookie.

Examples

Display TCP traffic statistics.

```
<Sysname> display tcp statistics
Received packets:
    Total: 4150
    packets in sequence: 1366 (134675 bytes)
    window probe packets: 0, window update packets: 0
    checksum error: 0, offset error: 0, short error: 0
    packets dropped for lack of memory: 0
    packets dropped due to PAWS: 0
    duplicate packets: 12 (36 bytes), partially duplicate packets: 0 (0 bytes)
    out-of-order packets: 0 (0 bytes)
    packets with data after window: 0 (0 bytes)
    packets after close: 0
    ACK packets: 3531 (795048 bytes)
    duplicate ACK packets: 33, ACK packets for unsent data: 0

Sent packets:
    Total: 4058
    urgent packets: 0
    control packets: 50
    window probe packets: 3, window update packets: 11
    data packets: 3862 (795012 bytes), data packets retransmitted: 0 (0 bytes)
    ACK-only packets: 150 (52 delayed)
    unnecessary packet retransmissions: 0

Syncache/syncookie related statistics:
    entries added to syncache: 12
    syncache entries retransmitted: 0
    duplicate SYN packets: 0
    reply failures: 0
    successfully build new socket: 12
    bucket overflows: 0
    zone failures: 0
    syncache entries removed due to RST: 0
    syncache entries removed due to timed out: 0
    ACK checked by syncache or syncookie failures: 0
    syncache entries aborted: 0
```

```
    syncache entries removed due to bad ACK: 0
    syncache entries removed due to ICMP unreachable: 0
    SYN cookies sent: 0
    SYN cookies received: 0

SACK related statistics:
    SACK recoveries: 1
    SACK retransmitted segments: 0 (0 bytes)
    SACK blocks (options) received: 0
    SACK blocks (options) sent: 0
    SACK scoreboard overflows: 0

Other statistics:
    retransmitted timeout: 0, connections dropped in retransmitted timeout: 0
    persist timeout: 0
    keepalive timeout: 21, keepalive probe: 0
    keepalive timeout, so connections disconnected: 0
    fin_wait_2 timeout, so connections disconnected: 0
    initiated connections: 29, accepted connections: 12, established connections:
23
    closed connections: 50051 (dropped: 0, initiated dropped: 0)
    bad connection attempt: 0
    ignored RSTs in the window: 0
    listen queue overflows: 0
    RTT updates: 3518(attempt segment: 3537)
    correct ACK header predictions: 0
    correct data packet header predictions: 568
    resends due to MTU discovery: 0
    packets dropped due to MD5 authentication failure: 0
    packets that passed MD5 authentication: 0
    sent Keychain-encrypted packets: 0
    packets that passed Keychain authentication: 0
    packets dropped due to Keychain authentication failure: 0
```

Related commands

reset tcp statistics

display tcp verbose

Use **display tcp verbose** to display detailed information about TCP connections.

Syntax

display tcp verbose [**slot** *slot-number* [**pcb** *pcb-index*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

pcb *pcb-index*: Displays detailed TCP connection information for the specified PCB. The index is a hexadecimal string in the range of 1 to ffffffffffffffff.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays detailed information about TCP connections for all member devices.

Usage guidelines

The detailed TCP connection information includes socket creator, state, option, type, protocol number, source IP address and port number, destination IP address and port number, and connection state.

Examples

Display detailed information about TCP connections.

```
<Sysname> display tcp verbose
TCP inpcb number: 1(tcpcb number: 1)

 Connection info: src = 192.168.20.200:179 ,  dst = 192.168.20.14:4181
 Location: slot 6 cpu 0
 NSR standby: N/A
 Creator: bgpd[199]
 State: ISCONNECTED
 Options: N/A
 Error: 0
 Receiving buffer(cc/hiwat/lowat/state): 0 / 65700 / 1 / N/A
 Sending buffer(cc/hiwat/lowat/state): 0 / 65700 / 512 / N/A
 Type: 1
 Protocol: 6
 Inpcb flags: N/A
 Inpcb extflag: N/A
 Inpcb vflag: INP_IPV4
 TTL: 255(minimum TTL: 0)
 Connection state: ESTABLISHED
 TCP options: TF_REQ_SCALE TF_REQ_TSTMP TF_SACK_PERMIT TF_NSR
 NSR state: READY(M)
 Send VRF: 0x0
 Receive VRF: 0x0
```

Table 5 Command output

Field	Description
TCP inpcb number	Number of TCP IP PCBs.
Connection info	Connection information, including source IP address, source port number, destination IP address, and destination port number.
Location	Socket location. This field is not available on the centralized devices.
tcpcb number	Number of TCP PCBs. This field is not displayed if the state of the TCP connection is **TIME_WAIT**.
Creator	Name of the operation that created the socket. The number in brackets is the process number of the creator.

Field	Description
State	State of the socket.
Options	Socket options.
Error	Error code.

Receiving buffer (cc/hiwat/lowat/state)	Displays receive buffer information in the following order:
	• **cc**—Used space.
	• **hiwat**—Maximum space.
	• **lowat**—Minimum space.
	• **state**—Buffer state:
	  ○ **CANTSENDMORE**—Unable to send data to the peer.
	  ○ **CANTRCVMORE**—Unable to receive data from the peer.
	  ○ **RCVATMARK**—Receiving tag.
	  ○ **N/A**—None of the above states.

Sending buffer (cc/hiwat/lowat/state)	Displays send buffer information in the following order:
	• **cc**—Used space.
	• **hiwat**—Maximum space.
	• **lowat**—Minimum space.
	• **state**—Buffer state:
	  ○ **CANTSENDMORE**—Unable to send data to the peer.
	  ○ **CANTRCVMORE**—Unable to receive data from the peer.
	  ○ **RCVATMARK**—Receiving tag.
	  ○ **N/A**—None of the above states.

Type	Socket type: • **1**—**SOCK_STREAM**. This socket uses TCP to provide reliable transmission of byte streams. • **2**—**SOCK_DGRAM**. This socket uses UDP to provide datagram transmission. • **3**—**SOCK_RAW**. This socket allows an application to change the next upper-layer protocol header. • **N/A**—None of the above types.
Protocol	Number of the protocol using the socket.

Field	Description
Inpcb flags	Flags in the Internet PCB: • **INP_RECVOPTS**—Receives IP options. • **INP_RECVRETOPTS**—Receives replied IP options. • **INP_RECVDSTADDR**—Receives destination IP address. • **INP_HDRINCL**—Provides the entire IP header. • **INP_REUSEADDR**—Reuses the IP address. • **INP_REUSEPORT**—Reuses the port number. • **INP_ANONPORT**—Port number not specified. • I**NP_RECVIF**—Records the input interface of the packet. • **INP_RECVTTL**—Receives TTL of the packet. Only UDP and RawIP support this flag. • **INP_DONTFRAG**—Sets the **Don't Fragment** flag. • **INP_ROUTER_ALERT**—Receives packets with the router alert option. Only RawIP supports this flag. • **INP_PROTOCOL_PACKET**—Identifies a protocol packet. • **INP_RCVVLANID**—Receives the VLAN ID of the packet. Only UDP and RawIP support this flag. • **INP_RCVMACADDR**—Receives the MAC address of the frame. • **INP_RECVTOS**—Receives TOS of the packet. Only UDP and RawIP support this flag. • **INP_SYNCPCB**—Waits until Internet PCB is synchronized. • **N/A**—None of the above flags.
Inpcb extflag	Extension flags in the Internet PCB: • **INP_EXTRCVPVCIDX**—Records the PVC index of the received packet. • **INP_RCVPWID**—Records the PW ID of the received packet. • **INP_EXTDONTDROP**—Does not drop the received packet. • **N/A**—None of the above flags.
Inpcb vflag	IP version flags in the Internet PCB: • **INP_IPV4**—IPv4 protocol. • **INP_TIMEWAIT**—In **TIMEWAIT** state. • **INP_ONESBCAST**—Sends broadcast packets. • **INP_DROPPED**—Protocol dropped flag. • **INP_SOCKREF**—Strong socket reference. • **INP_DONTBLOCK**—Do not block synchronization of the Internet PCB. • **N/A**—None of the above flags.
TTL	TTL value in the Internet PCB.

Field	Description
TCP options	TCP options: • **TF_MD5SIG**—Enables MD5 signature. • **TF_NODELAY**—Disables the Nagle algorithm that buffers the sent data inside the TCP. • **TF_NOOPT**—No TCP options. • **TF_NOPUSH**—Forces TCP to delay sending any TCP data until a full sized segment is buffered in the TCP buffers. • **TF_BINDFOREIGNADDR**—Binds the peer IP address. • **TF_NSR**—Enables TCP NSR. • **TF_REQ_SCALE**—Enables the TCP window scale option. • **TF_REQ_TSTMP**—Enables the time stamp option. • **TF_SACK_PERMIT**—Enables the TCP selective acknowledgement option. • **TF_ENHANCED_AUTH**—Enables the enhanced authentication option.
NSR state	State of the TCP connections. Between the parentheses is the role of the connection: • **M**—Main connection. • **S**—Standby connection.
Send VRF	This field is not supported in the current software version. VRF from which packets are sent.
Receive VRF	This field is not supported in the current software version. VRF from which packets are received.

display udp

Use **display udp** to display brief information about UDP connections.

Syntax

display udp [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays brief information about UDP connections for all member devices.

Usage guidelines

Brief UDP connection information includes local IP address and port number, and peer IP address and port number.

Examples

Display brief information about UDP connections.

```
<Sysname> display udp
```

```
Local Addr:port        Foreign Addr:port     Slot  PCB
0.0.0.0:69             0.0.0.0:0             1     0x0000000000000003
```

Table 6 Command output

Field	Description
Local Addr:port	Local IP address and port number.
Foreign Addr:port	Peer IP address and port number.
PCB	PCB index.

display udp statistics

Use **display udp statistics** to display UDP traffic statistics.

Syntax

display udp statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays UDP traffic statistics for all member devices.

Usage guidelines

UDP traffic statistics include information about received and sent UDP packets.

Examples

Display UDP traffic statistics.

```
<Sysname> display udp statistics
Received packets:
     Total: 240
     checksum error: 0, no checksum: 0
     shorter than header: 0, data length larger than packet: 0
     no socket on port(unicast): 0
     no socket on port(broadcast/multicast): 240
     not delivered, input socket full: 0
Sent packets:
     Total: 0
```

Related commands

reset udp statistics

display udp verbose

Use **display udp verbose** to display detailed information about UDP connections.

Syntax

display udp verbose [**slot** *slot-number* [**pcb** *pcb-index*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

pcb *pcb-index*: Displays detailed UDP connection information for the specified PCB. The index is a hexadecimal string in the range of 1 to ffffffffffffffff.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays detailed information about UDP connections for all member devices.

Usage guidelines

The detailed information includes socket creator, status, option, type, protocol number, source IP address and port number, and destination IP address and port number for UDP connections.

Examples

Display detailed UDP connection information.

```
<Sysname> display udp verbose
Total UDP socket number: 1

 Connection info: src = 0.0.0.0:69, dst = 0.0.0.0:0
 Location: slot 6 cpu 0
 Creator: sock_test_mips[250]
 State: N/A
 Options: N/A
 Error: 0
 Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 41600 / 1 / 0 / N/A
 Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A
 Type: 2
 Protocol: 17
 Inpcb flags: N/A
 Inpcb extflag: N/A
 Inpcb vflag: INP_IPV4
 TTL: 255(minimum TTL: 0)
 Send VRF: 0xffff
 Receive VRF: 0xffff
```

Table 7 Command output

Field	Description
Total UDP socket number	Total number of UDP sockets.
Connection info	Connection information, including source IP address, source port number, destination IP address, and destination port number.
Location	Socket location. This field is not available on the centralized devices.

Field	Description
Creator	Name of the operation that created the socket. The number in brackets is the process number of the creator.
State	Socket state.
Options	Socket option.
Error	Error code.

Receiving buffer(cc/hiwat/lowat/drop/state)	Displays receive buffer information in the following order:
	• **cc**—Used space.
	• **hiwat**—Maximum space.
	• **lowat**—Minimum space.
	• **drop**—Number of dropped packets.
	• **state**—Buffer state:
	  ○ **CANTSENDMORE**—Unable to send data to the peer.
	  ○ **CANTRCVMORE**—Unable to receive data from the peer.
	  ○ **RCVATMARK**—Receiving tag.
	  ○ **N/A**—None of the above states.

Sending buffer(cc/hiwat/lowat/state)	Displays send buffer information in the following order:
	• **cc**—Used space.
	• **hiwat**—Maximum space.
	• **lowat**—Minimum space.
	• **state**—Buffer state:
	  ○ **CANTSENDMORE**—Unable to send data to the peer.
	  ○ **CANTRCVMORE**—Unable to receive data from the peer.
	  ○ **RCVATMARK**—Receiving tag.
	  ○ **N/A**—None of the above states.

Type	Socket type: • **1**—**SOCK_STREAM**. This socket uses TCP to provide reliable transmission of byte streams. • **2**—**SOCK_DGRAM**. This socket uses UDP to provide datagram transmission. • **3**—**SOCK_RAW**. This socket allows an application to change the next upper-layer protocol header. • **N/A**—None of the above types.
Protocol	Number of the protocol using the socket.

Field	Description
Inpcb flags	Flags in the Internet PCB: • **INP_RECVOPTS**—Receives IP options. • **INP_RECVRETOPTS**—Receives replied IP options. • **INP_RECVDSTADDR**—Receives destination IP address. • **INP_HDRINCL**—Provides the entire IP header. • **INP_REUSEADDR**—Reuses the IP address. • **INP_REUSEPORT**—Reuses the port number. • **INP_ANONPORT**—Port number not specified. • I**NP_RECVIF**—Records the input interface of the packet. • **INP_RECVTTL**—Receives TTL of the packet. Only UDP and RawIP support this flag. • **INP_DONTFRAG**—Sets the **Don't Fragment** flag. • **INP_ROUTER_ALERT**—Receives packets with the router alert option. Only RawIP supports this flag. • **INP_PROTOCOL_PACKET**—Identifies a protocol packet. • **INP_RCVVLANID**—Receives the VLAN ID of the packet. Only UDP and RawIP support this flag. • **INP_RCVMACADDR**—Receives the MAC address of the frame. • **INP_RECVTOS**—Receives TOS of the packet. Only UDP and RawIP support this flag. • **INP_SYNCPCB**—Waits until Internet PCB is synchronized. • **N/A**—None of the above flags.
Inpcb extflag	Extension flags in the Internet PCB: • **INP_EXTRCVPVCIDX**—Records the PVC index of the received packet. • **INP_RCVPWID**—Records the PW ID of the received packet. • **N/A**—None of the above flags.
Inpcb vflag	IP version flags in the Internet PCB: • **INP_IPV4**—IPv4 protocol. • **INP_TIMEWAIT**—In **TIMEWAIT** state. • **INP_ONESBCAST**—Sends broadcast packets. • **INP_DROPPED**—Protocol dropped flag. • **INP_SOCKREF**—Strong socket reference. • **INP_DONTBLOCK**—Do not block synchronization of the Internet PCB. • **N/A**—None of the above flags.
TTL	TTL value in the Internet PCB.
Send VRF	This field is not supported in the current software version. VRF from which packets are sent.
Receive VRF	This field is not supported in the current software version. VRF from which packets are received.

ip forward-broadcast

Use **ip forward-broadcast** to enable an interface to forward directed broadcast packets destined for the directly connected network.

Use **undo ip forward-broadcast** to disable an interface from forwarding directed broadcast packets destined for the directly connected network.

Syntax

ip forward-broadcast [**acl** *acl-number*]

undo ip forward-broadcast

Default

An interface cannot forward directed broadcasts destined for the directly connected network.

Views

Interface view

Predefined user roles

network-admin

Parameters

acl *acl-number*: Specifies an ACL by its number. The interface forwards only the directed broadcasts permitted by the ACL. The value range for basic ACLs is 2000 to 2999. The value range for advanced ACLs is 3000 to 3999.

Usage guidelines

A directed broadcast packet is destined for all hosts on a specific network. In the destination IP address of the directed broadcast, the network ID identifies the target network, and the host ID is made up of all ones.

If an interface is allowed to forward directed broadcasts destined for the directly connected network, hackers can exploit this vulnerability to attack the target network. In some scenarios, however, an interface must send such directed broadcast packets to support UDP helper and Wake on LAN.

The command enables the interface to forward directed broadcast packets that are destined for the directly connected network and are received from another subnet to support Wake on LAN. Wake on LAN sends the directed broadcasts to wake up the hosts on the target network.

Examples

Enable VLAN-interface 2 to forward directed broadcast packets destined for the directly connected network.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ip forward-broadcast
```

ip icmp error-interval

Use **ip icmp error-interval** to set the interval for tokens to arrive in the bucket and the bucket size for ICMP error messages.

Use **undo ip icmp error-interval** to restore the default.

Syntax

ip icmp error-interval *interval* [*bucketsize*]

undo ip icmp error-interval

Default

A token is placed in the bucket every 100 milliseconds, and the bucket allows a maximum of 10 tokens.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the interval for tokens to arrive in the bucket. The value range is 0 to 2147483647 milliseconds. To disable the ICMP rate limit, set the value to 0.

bucketsize: Specifies the maximum number of tokens allowed in the bucket. The value range is 1 to 200.

Usage guidelines

This command limits the rate at which ICMP error messages are sent. Use this command to avoid sending excessive ICMP error messages within a short period that might cause network congestion. A token bucket algorithm is used with one token representing one ICMP error message.

A token is placed in the bucket at intervals until the maximum number of tokens that the bucket can hold is reached.

A token is removed from the bucket when an ICMP error message is sent. When the bucket is empty, ICMP error messages are not sent until a new token is placed in the bucket.

Examples

Set the interval to 200 milliseconds for tokens to arrive in the bucket and the bucket size to 40 tokens for ICMP error messages.

```
<Sysname> system-view
[Sysname] ip icmp error-interval 200 40
```

ip icmp receive enable

Use **ip icmp receive enable** to enable the device to receive a specific type of ICMP messages.

Use **undo ip icmp receive enable** to disable the device from receiving a specific type of ICMP messages.

NOTE:

This command is supported only in R6348P01 and later.

Syntax

ip icmp { **name** *icmp-name* | **type** *icmp-type* **code** *icmp-code* } **receive enable**

undo ip icmp { **name** *icmp-name* | **type** *icmp-type* **code** *icmp-code* } **receive enable**

Default

The device can receive all types of ICMP messages.

Views

System view

Predefined user roles

network-admin

Parameters

name *icmp-name*: Specifies an ICMP message name, a case-insensitive string of 1 to 20 characters.

type *icmp-type*: Specifies an ICMP message type. The value range for the *icmp-type* argument is 0 to 255.

code *icmp-code*: Specifies an ICMP message code. The value range for the *icmp-code* argument is 0 to 255.

Usage guidelines

CAUTION:

Disabling receiving ICMP messages of a specific type might affect network operation. Please use this feature with caution.

By default, the device receives all types of ICMP messages. Such a setting might affect device performance if a large number of ICMP responses are received within a short time. To solve this issue, you can use this command to disable the device from receiving a specific type of ICMP messages.

Table 8 shows common ICMP messages and their meanings.

Table 8 Common ICMP messages

Name	Type	Code	Description
echo	8	0	Echo request used to ping a target node.
echo-reply	0	0	Echo reply sent by a target node after receiving an echo request.
fragmentneed-dfset	3	4	Packets that need fragmentation but have the DF bit set.
host-redirect	5	1	Host redirection.
host-tos-redirect	5	3	Host ToS redirection.
host-unreachable	3	1	Unreachable host.
information-reply	16	0	Information reply.
information-request	15	0	Information request.
net-redirect	5	0	Network redirection.
net-tos-redirect	5	2	Network ToS redirection.
net-unreachable	3	0	Unreachable network.
parameter-problem	12	0	Invalid parameter.
port-unreachable	3	3	Unreachable port.
protocol-unreachable	3	2	Unreachable protocol.
reassembly-timeout	11	1	Fragment reassembly timeout.
source-quench	4	0	Source quench message.
source-route-failed	3	5	Source route failure.
timestamp-reply	14	0	Timestamp reply.
timestamp-request	13	0	Timestamp request.
ttl-exceeded	11	0	TTL exceeded in transit.

Examples

Enable the device to receive ICMP echo reply messages.

```
<Sysname> system-view
[Sysname] ip icmp name echo-reply receive enable
```

ip icmp send enable

Use **ip icmp send enable** to enable the device to send a specific type of ICMP messages.

Use **undo ip icmp send enable** to disable the device from sending a specific type of ICMP messages.

NOTE:

This command is supported only in R6348P01 and later.

Syntax

ip icmp { **name** *icmp-name* | **type** *icmp-type* **code** *icmp-code* } **send enable**

undo ip icmp { **name** *icmp-name* | **type** *icmp-type* **code** *icmp-code* } **send enable**

Default

The device sends all types of ICMP messages except Destination Unreachable, Time Exceeded, and Redirect messages.

Views

System view

Predefined user roles

network-admin

Parameters

name *icmp-name*: Specifies an ICMP message name, a case-insensitive string of 1 to 20 characters.

type *icmp-type*: Specifies an ICMP message type. The value range for the *icmp-type* argument is 0 to 255.

code *icmp-code*: Specifies an ICMP message code. The value range for the *icmp-code* argument is 0 to 255.

Usage guidelines

CAUTION:

Disabling sending ICMP messages of a specific type might affect network operation. Please use this feature with caution.

By default, the device sends all types of ICMP messages except Destination Unreachable, Time Exceeded, and Redirect messages. Attackers might obtain information from specific types of ICMP messages, causing security issues.

For security purposes, you can use this command to disable the device from sending ICMP messages of specific types.

To enable sending Destination Unreachable, Time Exceeded, or Redirect messages, you can perform one of the following tasks:

- Execute the **ip icmp send enable** command.
- Execute one of the following commands as needed:
  - **ip unreachables enable**
  - **ip ttl-expires enable**
  - **ip redirects enable**

Table 8 shows common ICMP messages and their meanings.

Examples

Enable the device to send ICMP echo reply messages.

```
<Sysname> system-view
[Sysname] ip icmp name echo-reply send enable
```

ip icmp source

Use **ip icmp source** to specify the source address for outgoing ICMP packets.

Use **undo ip icmp source** to remove the specified source address for outgoing ICMP packets.

Syntax

ip icmp source *ip-address*

undo ip icmp source

Default

No source address is specified for outgoing ICMP packets. The default source IP addresses for different types of ICMP packets vary as follows:

- For an ICMP error message, the source IP address is the IP address of the receiving interface of the packet that triggers the ICMP error message. ICMP error messages include Time Exceeded, Port Unreachable, and Parameter Problem messages.
- For an ICMP echo request, the source IP address is the IP address of the sending interface.
- For an ICMP echo reply, the source IP address is the destination IP address of the ICMP echo request specific to this reply.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies an IP address.

Usage guidelines

It is a good practice to specify the IP address of the loopback interface as the source IP address for outgoing ping echo request and ICMP error messages. This feature helps users to locate the sending device easily.

Examples

Specify 1.1.1.1 as the source address for outgoing ICMP packets.

```
<Sysname> system-view
[Sysname] ip icmp source 1.1.1.1
```

ip mtu

Use **ip mtu** to set the interface MTU for IPv4 packets. The setting defines the largest size of an IPv4 packet that an interface can transmit without fragmentation.

Use **undo ip mtu** to restore the default.

Syntax

ip mtu *mtu-size*

undo ip mtu

Default

The interface MTU is not set.

Views

Interface view

Predefined user roles

network-admin

Parameters

mtu-size: Specifies the MTU in bytes. The value range for the *mtu-size* argument is 128 to 1500.

Usage guidelines

When a packet exceeds the MTU of the sending interface, the device processes the packet in one of the following ways:

- If the packet disallows fragmentation, the device discards it.
- If the packet allows fragmentation, the device fragments it and forwards the fragments.

Fragmentation and reassembling consume system resources, so set an appropriate MTU to avoid fragmentation.

If an interface supports both the **mtu** and **ip mtu** commands, the device fragments a packet based on the MTU set by the **ip mtu** command.

Examples

Set the interface MTU for IPv4 packets to 1280 bytes on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ip mtu 1280
```

ip reassemble local enable

Use **ip reassemble local enable** to enable IPv4 local fragment reassembly.

Use **undo ip reassemble local enable** to disable local fragment reassembly.

Syntax

ip reassemble local enable

undo ip reassemble local enable

Default

IPv4 local fragment reassembly is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Use this feature on a multichassis IRF fabric to improve fragment reassembly efficiency. This feature enables a subordinate to reassemble the IPv4 fragments of a packet if all the fragments arrive at it. If

this feature is disabled, all IPv4 fragments are delivered to the master device for reassembly. The feature applies only to fragments destined for the same subordinate.

Examples

Enable IPv4 local fragment reassembly.

```
<Sysname> system-view
[Sysname] ip reassemble local enable
```

ip redirects enable

Use **ip redirects enable** to enable sending ICMP redirect messages.

Use **undo ip redirects enable** to disable sending ICMP redirect messages.

Syntax

ip redirects enable

undo ip redirects enable

Default

Sending ICMP redirect messages is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

ICMP redirect messages simplify host management and enable hosts to gradually optimize their routing tables.

A host that has only one route destined for the default gateway sends all packets to the default gateway. The default gateway sends an ICMP redirect message to inform the host of a correct next hop by following these rules:

- The receiving and sending interfaces are the same.
- The packet source IP address and the IP address of the packet receiving interface are on the same segment.
- There is no source route option in the received packet.

Examples

Enable sending ICMP redirect messages.

```
<Sysname> system-view
[Sysname] ip redirects enable
```

ip ttl-expires enable

Use **ip ttl-expires enable** to enable sending ICMP time exceeded messages.

Use **undo ip ttl-expires enable** to disable sending ICMP time exceeded messages.

Syntax

ip ttl-expires enable

undo ip ttl-expires enable

Default

Sending ICMP time exceeded messages is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

A device sends ICMP time exceeded messages by following these rules:

- The device sends an ICMP TTL exceeded in transit message to the source when the following conditions are met:
  - The received packet is not destined for the device.
  - The TTL field of the packet is 1.
- When the device receives the first fragment of an IP datagram destined for the device itself, it starts a timer. If the timer expires before all the fragments of the datagram are received, the device sends an ICMP fragment reassembly time exceeded message to the source.

A device disabled from sending ICMP time exceeded messages does not send ICMP TTL exceeded in transit messages but can still send ICMP fragment reassembly time exceeded messages.

Examples

Enable sending ICMP time exceeded messages.

```
<Sysname> system-view
[Sysname] ip ttl-expires enable
```

ip unreachables enable

Use **ip unreachables enable** to enable sending ICMP destination unreachable messages.

Use **undo ip unreachables enable** to disable sending ICMP destination unreachable messages.

Syntax

ip unreachables enable

undo ip unreachables enable

Default

Sending ICMP destination unreachable messages is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

A device sends ICMP destination unreachable messages by following these rules:

- The device sends the source an ICMP network unreachable message when the following conditions are met:
  - The received packet does not match any route.
  - No default route exists in the routing table.

- The device sends the source an ICMP protocol unreachable message when the following conditions are met:
  - The received packet is destined for the device.
  - The transport layer protocol of the packet is not supported by the device.
- The device sends the source an ICMP port unreachable message when the following conditions are met:
  - The received UDP packet is destined for the device.
  - The packet's port number does not match the running process.
- The device sends the source an ICMP source route failed message when the following conditions are met:
  - The source uses Strict Source Routing to send packets.
  - The intermediate device finds that the next hop specified by the source is not directly connected.
- The device sends the source an ICMP fragmentation needed and DF set message when the following conditions are met:
  - The MTU of the sending interface is smaller than the packet.
  - The packet has Don't Fragment set.

Examples

Enable sending ICMP destination unreachable messages.

```
<Sysname> system-view
[Sysname] ip unreachables enable
```

reset ip statistics

Use **reset ip statistics** to clear IP traffic statistics.

Syntax

reset ip statistics [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears IP traffic statistics for all member devices.

Usage guidelines

Use this command to clear history IP traffic statistics before you collect IP traffic statistics for a time period.

Examples

Clear IP traffic statistics.

```
<Sysname> reset ip statistics
```

Related commands

display ip interface

display ip statistics

reset tcp statistics

Use **reset tcp statistics** to clear TCP traffic statistics.

Syntax

reset tcp statistics

Views

User view

Predefined user roles

network-admin

Examples

Clear TCP traffic statistics.

```
<Sysname> reset tcp statistics
```

Related commands

display tcp statistics

reset udp statistics

Use **reset udp statistics** to clear UDP traffic statistics.

Syntax

reset udp statistics

Views

User view

Predefined user roles

network-admin

Examples

Clear UDP traffic statistics.

```
<Sysname> reset udp statistics
```

Related commands

display udp statistics

tcp mss

Use **tcp mss** to set the TCP maximum segment size (MSS).

Use **undo tcp mss** to restore the default.

Syntax

tcp mss *value*

undo tcp mss

Default

The TCP MSS is not set.

Views

Interface view

Predefined user roles

network-admin

Parameters

value: Specifies the TCP MSS in bytes. The value range for this argument is 128 to 1460.

Usage guidelines

The MSS option informs the receiver of the largest segment that the sender can accept. Each end announces its MSS during TCP connection establishment. If the size of a TCP segment is smaller than the MSS of the receiver, TCP sends the TCP segment without fragmentation. If not, TCP fragments the segment according to the receiver's MSS.

If you set the TCP MSS on an interface, the size of each TCP segment received or sent on the interface cannot exceed the MSS value.

This configuration takes effect only on TCP connections that are established after the configuration and not on the TCP connections that already exist.

This configuration is effective only on IP packets.

Examples

Set the TCP MSS to 300 bytes on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] tcp mss 300
```

tcp path-mtu-discovery

Use **tcp path-mtu-discovery** to enable TCP path MTU discovery.

Use **undo tcp path-mtu-discovery** to disable TCP path MTU discovery.

Syntax

tcp path-mtu-discovery [**aging** *age-time* | **no-aging**]

undo tcp path-mtu-discovery

Default

TCP path MTU discovery is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

aging *age-time*: Specifies the aging time for the path MTU, in the range of 10 to 30 minutes. The default aging time is 10 minutes.

no-aging: Does not age out the path MTU.

Usage guidelines

After you enable TCP path MTU discovery, all new TCP connections detect the path MTU. The device uses the path MTU to calculate the MSS to avoid IP fragmentation.

After you disable TCP path MTU discovery, the system stops all path MTU timers. The TCP connections established later do not detect the path MTU, but the TCP connections previously established still can detect the path MTU.

Examples

Enable TCP path MTU discovery and set the path MTU aging time to 20 minutes.

```
<Sysname> system-view
[Sysname] tcp path-mtu-discovery aging 20
```

tcp syn-cookie enable

Use **tcp syn-cookie enable** to enable SYN Cookie to protect the device from SYN flood attacks.

Use **undo tcp syn-cookie enable** to disable SYN Cookie.

Syntax

tcp syn-cookie enable

undo tcp syn-cookie enable

Default

SYN Cookie is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

A TCP connection is established through a three-way handshake:

1. The sender sends a SYN packet to the server.
2. The server receives the SYN packet, establishes a TCP semi-connection in SYN_RECEIVED state, and replies with a SYN ACK packet to the sender.
3. The sender receives the SYN ACK packet and replies with an ACK packet. Then, a TCP connection is established.

An attacker can exploit this mechanism to mount SYN flood attacks. The attacker sends a large number of SYN packets, but they do not respond to the SYN ACK packets from the server. As a result, the server establishes a large number of TCP semi-connections and cannot handle normal services.

SYN Cookie can protect the server from SYN flood attacks. When the server receives a SYN packet, it responds to the request with a SYN ACK packet without establishing a TCP semi-connection.

The server establishes a TCP connection and enters ESTABLISHED state only when it receives an ACK packet from the sender.

Examples

Enable SYN Cookie.

```
<Sysname> system-view
[Sysname] tcp syn-cookie enable
```

tcp timer fin-timeout

Use **tcp timer fin-timeout** to set the TCP FIN wait timer.

Use **undo tcp timer fin-timeout** to restore the default.

Syntax

tcp timer fin-timeout *time-value*

undo tcp timer fin-timeout

Default

The TCP FIN wait timer is 675 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

time-value: Specifies the TCP FIN wait timer in the range of 76 to 3600 seconds.

Usage guidelines

TCP starts the FIN wait timer when the state of a TCP connection changes to FIN_WAIT_2. If no FIN packet is received within the timer interval, the TCP connection is terminated.

If a FIN packet is received, TCP changes the connection state to TIME_WAIT. If a non-FIN packet is received, TCP restarts the timer and tears down the connection when the timer expires.

Examples

Set the TCP FIN wait timer to 800 seconds.

```
<Sysname> system-view
[Sysname] tcp timer fin-timeout 800
```

tcp timer syn-timeout

Use **tcp timer syn-timeout** to set the TCP SYN wait timer.

Use **undo tcp timer syn-timeout** to restore the default.

Syntax

tcp timer syn-timeout *time-value*

undo tcp timer syn-timeout

Default

The TCP SYN wait timer is 75 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

time-value: Specifies the TCP SYN wait timer in the range of 2 to 600 seconds.

Usage guidelines

TCP starts the SYN wait timer after sending a SYN packet. Within the SYN wait timer if no response is received or the upper limit on TCP connection tries is reached, TCP fails to establish the connection.

Examples

Set the TCP SYN wait timer to 80 seconds.

```
<Sysname> system-view
[Sysname] tcp timer syn-timeout 80
```

tcp timestamps enable

Use **tcp timestamps enable** to enable the device to encapsulate the TCP Timestamps option in outgoing TCP packets.

Use **undo tcp timestamps enable** to disable the device from encapsulating the TCP Timestamps option in outgoing TCP packets.

Syntax

tcp timestamps enable

undo tcp timestamps enable

Default

The TCP Timestamps option is encapsulated in outgoing TCP packets.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Devices at each end of the TCP connection can calculate the RTT value by using the TCP Timestamps option carried in TCP packets. For security purpose in some networks, you can disable the TCP Timestamps option encapsulation at one end of the TCP connection to prevent intermediate devices from obtaining the option information.

This command takes effect only on new connections that are established after you execute the command. Existing TCP connections are not affected.

Examples

Enable the device to encapsulate the TCP Timestamps option in outgoing TCP packets.

```
<Sysname> system-view
[Sysname] undo tcp timestamps enable
```

tcp window

Use **tcp window** to set the size of the TCP receive/send buffer.

Use **undo tcp window** to restore the default.

Syntax

tcp window *window-size*

undo tcp window

Default

The size of the TCP receive/send buffer is 63 KB.

Views

System view

Predefined user roles

network-admin

Parameters

window-size: Specifies the size of the TCP receive/send buffer, in the range of 1 to 64 KB.

Examples

Set the size of the TCP receive/send buffer to 3 KB.

```
<Sysname> system-view
[Sysname] tcp window 3
```

Contents

UDP helper commands

The following switch series do not support UDP helper:

- S5110V2-SI.
- S5000V3-EI.
- S5000V5-EI.
- S5000E-X.
- S5000X-EI.
- WAS6000.

display udp-helper interface

Use **display udp-helper interface** to display information about broadcast to unicast conversion by UDP helper on an interface.

Syntax

display udp-helper interface *interface-type interface-number*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

This command displays information about destination servers and total number of unicast packets converted from UDP broadcast packets by UDP helper.

Examples

Display information about broadcast to unicast conversion by UDP helper on VLAN-interface 100.

```
<Sysname> display udp-helper interface vlan-interface 100
Interface               Server VPN instance          Server address Packets sent
Vlan-interface100       N/A                          192.1.1.2      0
```

Table 1 Command output

Field	Description
Interface	Interface name.
Server VPN instance	This field is not supported in the current software version. VPN instance to which the destination server belongs.
Server address	Destination server to which UDP packets are forwarded.
Packets sent	Number of unicast packets that are converted from broadcast packets by UDP helper.

Related commands

reset udp-helper statistics

udp-helper server

reset udp-helper statistics

Use **reset udp-helper statistics** to clear statistics about broadcast to unicast conversion by UDP helper.

Syntax

reset udp-helper statistics

Views

User view

Predefined user roles

network-admin

Examples

Clear the statistics about broadcast to unicast conversion by UDP helper.

```
<Sysname> reset udp-helper statistics
```

Related commands

display udp-helper interface

udp-helper broadcast-map

Use **udp-helper broadcast-map** to specify a multicast address for UDP helper to convert broadcast to multicast.

Use **undo udp-helper broadcast-map** to restore the default.

Syntax

udp-helper broadcast-map *multicast-address* [**acl** *acl-number*]

undo udp-helper broadcast-map *multicast-address*

Default

No multicast address is specified for UDP helper to convert broadcast to multicast.

Views

Interface view

Predefined user roles

network-admin

Parameters

multicast-address: Specifies the destination multicast address to which the destination broadcast address is converted.

acl *acl-number*: Specifies an ACL by its number. The ACL filters incoming broadcast packets for UDP helper. Packets permitted by the ACL can be converted. If no ACL is specified, all incoming broadcast packets are checked for UDP helper.

- For a basic ACL, the value range is 2000 to 2999.
- For an advanced ACL, the value range is 3000 to 3999.

Usage guidelines

Use this command on the interface that receives broadcast packets.

You can configure a maximum of 20 unicast and multicast addresses for UDP helper to convert broadcast packets.

Examples

Configure UDP helper to convert received broadcast packets on VLAN-interface 100 to multicast packets destined for 225.0.0.1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] udp-helper broadcast-map 225.0.0.1
```

udp-helper enable

Use **udp-helper enable** to enable UDP helper.

Use **undo udp-helper enable** to disable UDP helper.

Syntax

udp-helper enable

undo udp-helper enable

Default

UDP helper is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

For UDP helper to take effect on an interface, make sure the following conditions are met:

- UDP helper is enabled.
- A UDP port number is specified by using the **udp-helper port** command.
- Packet conversion for UDP helper is configured on the interface.

Examples

Enable UDP helper.

```
<Sysname> system-view
[Sysname] udp-helper enable
```

Related commands

udp-helper port

udp-helper server

udp-helper broadcast-map

udp-helper port

Use **udp-helper port** to specify a UDP port number for UDP helper.

Use **undo udp-helper port** to remove UDP port numbers.

Syntax

udp-helper port { *port-number* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }

undo udp-helper port { *port-number* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }

Default

No UDP port numbers are specified for UDP helper.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies a UDP port number in the range of 1 to 65535 (except 67 and 68).

dns: Specifies the UDP port 53 used by DNS packets.

netbios-ds: Specifies the UDP port 138 used by NetBIOS distribution service packets.

netbios-ns: Specifies the UDP port 137 used by NetBIOS name service packets.

tacacs: Specifies the UDP port 49 used by TACACS packets.

tftp: Specifies the UDP port 69 used by TFTP packets.

time: Specifies the UDP port 37 used by time protocol packets.

Usage guidelines

Upon receiving a UDP broadcast or multicast packet, UDP helper uses the specified UDP ports to match the UDP destination port number of the packet.

To specify a UDP port, you can specify the port number or the protocol keyword. For example, **udp-helper port** 53 and **udp-helper port dns** specify the same UDP port.

You can specify a maximum of 256 UDP ports on a device.

Examples

Specify the UDP port 100 for UDP helper.

```
<Sysname> system-view
[Sysname] udp-helper port 100
```

udp-helper server

Use **udp-helper server** to specify a destination server for UDP helper to convert broadcast to unicast.

Use **undo udp-helper server** to remove a destination server.

Syntax

udp-helper server *ip-address*

undo udp-helper server [*ip-address*]

Default

No destination server is specified for UDP helper to convert broadcast to unicast.

Views

Interface view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address of a destination server, in dotted decimal notation.

Usage guidelines

Specify destination servers on an interface that receives UDP broadcast packets. If the packets' destination UDP port numbers match the UDP helper ports, UDP helper forwards the broadcasts to the specified servers.

You can specify a maximum of 20 unicast and multicast addresses for UDP helper to convert broadcast packets on an interface.

If you do not specify the *ip-address* argument, the **undo udp-helper server** command removes all destination servers on the interface.

Examples

Specify the destination server 192.1.1.2 for UDP helper to convert broadcast to unicast on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] udp-helper server 192.1.1.2
```

Related commands

display udp-helper interface

Contents

IPv6 basics commands

display ipv6 fib

Use **display ipv6 fib** to display IPv6 FIB entries.

Syntax

display ipv6 fib [*ipv6-address* [*prefix-length*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6-address: Displays IPv6 FIB entries for a destination IPv6 address. If you do not specify an IPv6 address, this command displays all IPv6 FIB entries.

prefix-length: Specifies a prefix length for the IPv6 address, in the range of 0 to 128. If you do not specify the prefix length, this command displays the IPv6 FIB entry longest matching the IPv6 address.

Examples

Display all IPv6 FIB entries.

```
<Sysname> display ipv6 fib

Destination count: 1 FIB entry count: 1

Flag:
  U:Usable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Relay    F:FRR

Destination: ::1                                    Prefix length: 128
Nexthop    : ::1                                    Flags: UH
Time stamp : 0x1                                    Label: Null
Interface  : InLoop0                                Token: Invalid
```

Table 1 Command output

Field	Description
Destination count	Total number of destination addresses.
FIB entry count	Total number of IPv6 FIB entries.
Destination	Destination address.
Prefix length	Prefix length of the destination address.
Nexthop	Next hop address.
Flags	Route flag: • **U**—Usable route.

Field	Description
	• **G**—Gateway route. • **H**—Host route. • **B**—Black hole route. • **D**—Dynamic route. • **S**—Static route. • **R**—Recursive route. • **F**—Fast re-route.
Time stamp	Time when the IPv6 FIB entry was generated.
Label	Inner MPLS label. For IPv6 FIB entries on the public network, this field displays **Null**.
Interface	Outgoing interface.
Token	Label switched path index number.

display ipv6 icmp statistics

Use **display ipv6 icmp statistics** to display ICMPv6 packet statistics.

Syntax

display ipv6 icmp statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays ICMPv6 packet statistics for all member devices.

Examples

Display ICMPv6 packet statistics.

```
<Sysname> display ipv6 icmp statistics
  Input: bad code              0         too short               0
         checksum error        0         bad length              0
         path MTU changed      0        destination unreachable  0
         too big               0        parameter problem        0
         echo request          0        echo reply               0
         neighbor solicit      0         neighbor advertisement  0
         router solicit        0        router advertisement     0
         redirect              0        router renumbering       0
 output: parameter problem     0         echo request            0
         echo reply            0         unreachable no route     0
         unreachable admin     0         unreachable beyond scope 0
         unreachable address   0        unreachable no port      0
         too big               0         time exceed transit     0
         time exceed reassembly 0         redirect                0
```

```
        ratelimited            0         other errors           0
```

display ipv6 interface

Use **display ipv6 interface** to display IPv6 interface information.

Syntax

display ipv6 interface [*interface-type* [*interface-number*]] [**brief**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type: Specifies an interface by its type.

interface-number: Specifies an interface by its number.

brief: Displays brief IPv6 interface information, including physical status, link-layer protocols, and IPv6 address. If you do not specify the keyword, this command displays detailed IPv6 interface information, including IPv6 configuration and operating information, and IPv6 packet statistics.

Usage guidelines

If you do not specify an interface, this command displays IPv6 information about all interfaces.

If you specify only the *interface-type* argument, this command displays IPv6 information about the interfaces of the specified type.

If you specify both the *interface-type* and the *interface-number* arguments, this command displays IPv6 information about the specified interface.

Examples

Display IPv6 information about VLAN-interface 2.

```
<Sysname> display ipv6 interface vlan-interface 2
Vlan-interface2 current state: UP
Line protocol current state: UP
IPv6 is enabled, link-local address is FE80::1234:56FF:FE65:4322/64 [TENTATIVE]
  Global unicast address(es):
    10::1234:56FF:FE65:4322, subnet is 10::/64 [TENTATIVE] [AUTOCFG]
      [valid lifetime 4641s/preferred lifetime 4637s]
    20::1234:56ff:fe65:4322, subnet is 20::/64 [TENTATIVE] [EUI-64]
    30::1, subnet is 30::/64 [TENTATIVE] [ANYCAST]
    40::2, subnet is 40::/64 [TENTATIVE] [DHCP]
    50::3, subnet is 50::/64 [TENTATIVE]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
    FF02::1:FF65:4322
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
```

```
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
IPv6 Packet statistics:
  InReceives:                0
  InTooShorts:               0
  InTruncatedPkts:           0
  InHopLimitExceeds:         0
  InBadHeaders:              0
  InBadOptions:              0
  ReasmReqds:                0
  ReasmOKs:                  0
  InFragDrops:               0
  InFragTimeouts:            0
  OutFragFails:              0
  InUnknownProtos:           0
  InDelivers:                0
  OutRequests:               0
  OutForwDatagrams:          0
  InNoRoutes:                0
  InTooBigErrors:            0
  OutFragOKs:                0
  OutFragCreates:            0
  InMcastPkts:               0
  InMcastNotMembers:         0
  OutMcastPkts:              0
  InAddrErrors:              0
  InDiscards:                0
  OutDiscards:               0
```

Table 2 Command output

Field	Description
Vlan-interface2 current state	Physical state of the interface: • **Administratively DOWN**—The interface has been administratively shut down by using the **shutdown** command. • **DOWN**—The interface is administratively up but its physical state is down, possibly because of a connection or link failure. • **UP**—The administrative and physical states of the interface are both up.
Line protocol current state	Link layer state of the interface: • **DOWN**—The link layer protocol state of the interface is down. • **UP**—The link layer protocol state of the interface is up.
IPv6 is enabled	IPv6 is enabled on the interface. This feature is automatically enabled after an IPv6 address is configured for an interface.
link-local address	Link-local address of the interface.
Global unicast address(es)	Global unicast addresses of the interface. IPv6 address states: • **TENTATIVE**—Initial state. DAD is being performed or is to be performed on the address.

Field	Description
	• **DUPLICATE**—The address is not unique on the link. • **PREFERRED**—The address is preferred and can be used as the source or destination address of a packet. If an address is in this state, the command does not display the address state. • **DEPRECATED**—The address is beyond the preferred lifetime but in the valid lifetime. It is valid, but it cannot be used as the source address for a new connection. Packets destined for the address are processed correctly. If a global unicast address is not manually configured, the following notations indicate how the address is obtained: • **AUTOCFG**—Stateless autoconfigured. • **DHCP**—Assigned by a DHCPv6 server. • **EUI-64**—Manually configured EUI-64 IPv6 address. • **RANDOM**—Random address automatically generated. If the address is a manually configured anycast address, it is noted with **ANYCAST**.
valid lifetime	Specifies how long autoconfigured global unicast addresses using a prefix are valid.
preferred lifetime	Specifies how long autoconfigured global unicast addresses using a prefix are preferred.
Joined group address(es)	Addresses of the multicast groups that the interface has joined.
MTU	MTU of the interface.
ND DAD is enabled, number of DAD attempts	DAD is enabled. • If DAD is enabled, this field displays the number of attempts to send an NS message for DAD (set by using the **`ipv6 nd dad attempts`** command). • If DAD is disabled, this field displays **ND DAD is disabled**. To disable DAD, set the number of attempts to 0.
ND reachable time	Time during which a neighboring device is reachable.
ND retransmit interval	Interval for retransmitting an NS message.
Hosts use stateless autoconfig for addresses	Hosts obtained IPv6 addresses through stateless autoconfiguration.
InReceives	Received IPv6 packets, including error messages.
InTooShorts	Received IPv6 packets that are too short. For example, the received IPv6 packet is less than 40 bytes.
InTruncatedPkts	Received IPv6 packets with a length less than the payload length field specified in the packet header.
InHopLimitExceeds	Received IPv6 packets with a hop count exceeding the hop limit field specified in the packet header.
InBadHeaders	Received IPv6 packets with incorrect basic headers.
InBadOptions	Received IPv6 packets with incorrect extension headers.
ReasmReqds	Received IPv6 fragments.
ReasmOKs	Number of reassembled IPv6 packets.
InFragDrops	Received IPv6 fragments that are discarded because of certain errors.
InFragTimeouts	Received IPv6 fragments that are discarded because the amount of time they stay in the system buffer exceeds the specified interval.

Field	Description
OutFragFails	IPv6 packets that fail to be fragmented on the output interface.
InUnknownProtos	Received IPv6 packets with unknown or unsupported protocol type.
InDelivers	Received IPv6 packets that are delivered to user protocols (such as ICMPv6, TCP, and UDP).
OutRequests	Local IPv6 packets sent by IPv6 user protocols.
OutForwDatagrams	IPv6 packets forwarded by the interface.
InNoRoutes	Received IPv6 packets that are discarded because no matching route can be found.
InTooBigErrors	Received IPv6 packets that fail to be forwarded because they exceeded the Path MTU.
OutFragOKs	Fragmented IPv6 packets on the output interface.
OutFragCreates	Number of IPv6 fragments on the output interface.
InMcastPkts	Received IPv6 multicast packets.
InMcastNotMembers	Received IPv6 multicast packets that are discarded because the interface is not in the multicast group.
OutMcastPkts	IPv6 multicast packets sent by the interface.
InAddrErrors	Received IPv6 packets that are discarded due to invalid destination addresses.
InDiscards	Received IPv6 packets that are discarded due to resource problems rather than packet errors.
OutDiscards	IPv6 packets that fail to be sent due to resource problems rather than packet errors.

Display brief IPv6 information about all interfaces.

```
<Sysname> display ipv6 interface brief
*down: administratively down
(s): spoofing
Interface                          Physical Protocol IPv6 Address
Vlan-interface1                    down    down     Unassigned
Vlan-interface2                    up        up     2001::1
Vlan-interface100                   up        up       Unassigned
```

Table 3 Command output

Field	Description
*down: administratively down	The interface has been administratively shut down by using the **shutdown** command.
(s): spoofing	Spoofing attribute of the interface. The link protocol state of the interface is up, but the link is temporarily established on demand or does not exist.
Interface	Name of the interface.
Physical	Physical state of the interface: • ***down**—The interface has been administratively shut down by using the **shutdown** command. • **down**—The interface is administratively up but its physical state is down, possibly because of a connection or link failure. • **up**—The administrative and physical states of the interface are both

Field	Description
	up.
Protocol	Link layer protocol state of the interface: • **down**—The network layer protocol state of the interface is down. • **up**—The network layer protocol state of the interface is up.
IPv6 Address	IPv6 address of the interface. • If multiple global unicast addresses are configured, this field displays the lowest address. • If no global unicast address is configured, this field displays the link-local address. • If no address is configured, this field displays **Unassigned**.

display ipv6 interface prefix

Use **display ipv6 interface prefix** to display IPv6 prefix information for an interface.

Syntax

display ipv6 interface *interface-type interface-number* **prefix**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Examples

Display IPv6 prefix information for VLAN-interface 10.

```
<Sysname> display ipv6 interface vlan-interface 10 prefix
Prefix: 1001::/65                                  Origin: ADDRESS
Age:    -                                           Flag:   AL
Lifetime(Valid/Preferred): 2592000/604800
Preference: -

Prefix: 2001::/64                                  Origin: STATIC
Age:    -                                           Flag:   L
Lifetime(Valid/Preferred): 3000/2000
Preference: -

Prefix: 3001::/64                                  Origin: RA
Age:    600                                         Flag:   A
Lifetime(Valid/Preferred): -
Preference: -

Prefix: 4001::/64                                  Origin: STATIC
Age:    -                                           Flag:   ALP
Lifetime(Valid/Preferred): 1000/200
```

```
Preference: 200
```

Table 4 Command output

Filed	Description
Prefix	IPv6 address prefix.
Origin	How the prefix is generated: • **STATIC**—Manually configured by using the **ipv6 nd ra prefix** command. • **RA**—Advertised in RA messages after stateless autoconfiguration is enabled. • **ADDRESS**—Generated by a manually configured address.
Age	Aging time in seconds. If the prefix does not age out, this field displays a hyphen (-).
Flag	Flags carried in RA messages. If no flags are available, this field displays a hyphen (-). • **L**—The address with the prefix is directly reachable on the link. • **A**—The prefix is used for stateless autoconfiguration. • **N**—The prefix is not advertised in RA messages. • **P**—The prefix has a preference.
Lifetime	Lifetime in seconds advertised in RA messages. If the prefix does not need to be advertised, this field displays a hyphen (-). • **Valid**—Valid lifetime of the prefix. • **Preferred**—Preferred lifetime of the prefix.
Preference	Preference of the IPv6 prefix.

Related commands

ipv6 nd ra prefix

display ipv6 nd snooping count vlan

Use **display ipv6 nd snooping count vlan** to display the number of IPv6 ND snooping entries for VLANs.

Syntax

display ipv6 nd snooping count vlan [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays the total number of ND snooping entries in all VLANs.

Examples

Display the total number of IPv6 ND snooping entries in all VLANs.

```
<Sysname> display ipv6 nd snooping count vlan
Total entries for VLANs: 5
```

Display the total number of IPv6 ND snooping entries on GigabitEthernet 1/0/1.

```
<Sysname> display ipv6 nd snooping count vlan interface gigabitethernet 1/0/1
Total entries on interface GE1/0/1: 2
```

Table 5 Command output

Field	Description
Total entries for VLANs	Total number of ND snooping entries in all VLANs.
Total entries on interface *xxx*	Total number of ND snooping entries on the interface.

Related commands

ipv6 nd snooping enable global

ipv6 nd snooping enable link-local

reset ipv6 nd snooping vlan

display ipv6 nd snooping vlan

Use **display ipv6 nd snooping vlan** to display ND snooping entries in the specified VLAN.

Syntax

display ipv6 nd snooping vlan [[*vlan-id* | **interface** *interface-type interface-number*] [**global** | **link-local**] | *ipv6-address*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan *vlan-id*: Displays ND snooping entries for the specified VLAN. The value range for the VLAN ID is 1 to 4094.

interface *interface-type interface-number*: Displays ND snooping entries for the specified interface in a VLAN. The *interface-type interface-number* argument specifies an interface by its type and number.

global: Displays ND snooping entries for global unicast addresses in the VLAN.

link-local: Displays ND snooping entries for link-local addresses in the VLAN.

ipv6-address: Displays the ND snooping entry for the specified IPv6 address.

verbose: Displays detailed information about ND snooping entries in the VLAN. If you do not specify the keyword, this command displays brief information about ND snooping entries.

Usage guidelines

If you do not specify any parameters, this command displays all ND snooping entries.

Examples

Display brief information about IPv6 ND snooping entries for VLAN 1.

```
<Sysname> display ipv6 nd snooping vlan 1
IPv6 address            MAC address    VID  Interface    Status      Age
1::2                    0000-1234-0c01  1   GE1/0/2      VALID       57
```

Display detailed information about IPv6 ND snooping entries for VLAN 1.

```
<Sysname> display ipv6 nd snooping vlan 1 verbose
IPv6 address: 1::2
MAC address: 0000-1234-0c01
Interface: GE1/0/2
First VLAN ID: 1   Second VLAN ID: N/A
Status: VALID   Age: 57
```

Table 6 Command output

Field	Description
IPv6 address	IPv6 address in the ND snooping entry.
MAC address	MAC address in the ND snooping entry.
VID	ID of the VLAN to which the ND snooping entry belongs.
First VLAN ID	ID of the SVLAN to which the ND snooping entry belongs.
Second VLAN ID	ID of the CVLAN to which the ND snooping entry belongs. If no CVLAN is configured, this field displays **N/A**. For more information about the SVLAN and CVLAN, see QinQ in *Layer 2—LAN Switching Configuration Guide*.
Interface	Input interface in the ND snooping entry.

Status	Status of the ND snooping entry:
	• **TENTATIVE**—The entry is ineffective.
	• **VALID**—The entry is effective.
	• **TESTING_TPLT**—The entry is being tested by DAD. The device performs DAD for the entry in the following situations:
	  ○ The entry ages out.
	  ○ An ND trusted interface in the VLAN receives an ND message from the IPv6 address in the entry.
	• **TESTING_VP**—The entry is being tested by DAD. The device performs DAD when an ND untrusted interface in the VLAN receives an ND message from the IPv6 address in the entry.

Age	For an ND snooping entry in VALID status, this field displays its remaining aging time in seconds. For an ND snooping entry in other status, this field displays a pound sign (#).

Related commands

ipv6 nd snooping enable global

ipv6 nd snooping enable link-local

display ipv6 nd user-ip-conflict record

Use **display ipv6 nd user-ip-conflict record** to display user IPv6 address conflict records.

Syntax

display ipv6 nd user-ip-conflict record [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays user IP address conflict records for all member devices.

Examples

Display all user IPv6 address conflict records.

```
<Sysname> display ipv6 nd user-ip-conflict record
IPv6 address: 10::1
System time: 2018-02-02 11:22:29
Conflict count: 1
Log suppress count: 0
Old interface: GigabitEthernet1/0/1
New interface: GigabitEthernet1/0/2
Old SVLAN/CVLAN: 100/2
New SVLAN/CVLAN: 100/2
Old MAC: 00e0-ca63-8141
New MAC: 00e0-ca63-8142

IPv6 address: 10::2
System time: 2018-02-02 10:20:30
Conflict count: 1
Log suppress count: 0
Old interface: GigabitEthernet1/0/1
New interface: GigabitEthernet1/0/2
Old SVLAN/CVLAN: 100/--
New SVLAN/CVLAN: 100/--
Old MAC: 00e0-ca63-8141
New MAC: 00e0-ca63-8142
```

Table 7 Command output

Field	Description
IPv6 address	IPv6 address of a user.
System time	Time when the user IPv6 address conflict occurred.
Conflict count	Number of times user IPv6 address conflicts occurred.
Log suppress count	Number of times user IPv6 address conflict log generation has been suppressed.
Old interface	Output interface in the old ND entry.
New interface	Output interface in the new ND entry.
Old SVLAN/CVLAN	ID of the outer VLAN or inner VLAN in the old ND entry. This field displays hyphens (**--**) if the ND entry does not belong to any outer VLAN or inner VLAN.
New SVLAN/CVLAN	ID of the outer VLAN or inner VLAN in the new ND entry. This field displays hyphens (**--**) if the ND entry does not belong to any outer VLAN or inner VLAN.
Old MAC	MAC address in the old ND entry.
New MAC	MAC address in the new ND entry.

Related commands

ipv6 nd user-ip-conflict record enable

display ipv6 nd user-move record

Use **display ipv6 nd user-move record** to display user port migration records.

Syntax

display ipv6 nd user-move record [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays user port migration records for all member devices.

Examples

Display all user port migration records.

```
<Sysname> display ipv6 nd user-move record
IPv6 address: 10::1
MAC address: 00e0-ca63-8141
System time: 2018-02-02 11:22:29
Move count: 1
Log suppress count: 0
Before:
  interface: GigabitEthernet1/0/1
  SVLAN/CVLAN: 100/2
After:
  interface: GigabitEthernet1/0/2
  SVLAN/CVLAN: 100/2

IPv6 address: 10::2
MAC address: 00e0-ca63-8142
System time: 2018-02-02 10:20:30
Move count: 1
Log suppress count: 0
Before:
  interface: GigabitEthernet1/0/1
  SVLAN/CVLAN: 100/--
After:
  interface: GigabitEthernet1/0/2
  SVLAN/CVLAN: 100/--
```

Table 8 Command output

Field	Description
IPv6 address	IPv6 address of the user.
MAC address	MAC address of the user.
System time	Time when the user port migration occurred.
Move count	Number of times the user port migrated.
Log suppress count	Number of times user port migration log generation has been suppressed.
Before	Information before the user port migration.
interface	Interface information in the ND entry.
SVLAN/CVLAN	ID of the outer VLAN or inner VLAN in the ND entry. This field displays hyphens (**--**) if the ND entry does not belong to any outer VLAN or inner VLAN.
After	Information after the user port migration.

Related commands

ipv6 nd user-move record enable

display ipv6 neighbors

Use **display ipv6 neighbors** to display IPv6 neighbor information.

Syntax

display ipv6 neighbors { { *ipv6-address* | **all** | **dynamic** | **static** } [**slot** *slot-number*] | **interface** *interface-type interface-number* | **vlan** *vlan-id* } [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6-address: Specifies the IPv6 address of a neighbor whose information is displayed.

all: Displays information about all neighbors, including neighbors acquired dynamically and configured statically.

dynamic: Displays information about all neighbors acquired dynamically.

static: Displays information about all neighbors configured statically.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 neighbor information for all member devices.

interface *interface-type interface-number*: Specifies an interface by its type and number.

vlan *vlan-id*: Displays information about neighbors in the specified VLAN. The value range for VLAN ID is 1 to 4094.

verbose: Displays detailed neighbor information.

Examples

Display all neighbor information.

```
<Sysname> display ipv6 neighbors all
Type: S-Static    D-Dynamic    O-Openflow    R-Rule    IS-Invalid static
IPv6 address              MAC address    VID  Interface        State T  Aging
1::2                   6864-6839-0202 1    GE1/0/1          STALE D  136
FE80::6A64:68FF:FE39:202  6864-6839-0202 1    GE1/0/1           STALE D  126
1::4                   6864-6839-0204 1    GE1/0/2          STALE D  136
```

Display detailed information about all neighbors.

```
<Sysname> display ipv6 neighbors all verbose
IPv6 Address    : 1::2
MAC address     : 6864-6839-0202          Type  : Dynamic
State           : STALE                   Aging : 136   seconds
Interface       : GE1/0/1                 VID   : 1
VPN instance    : --
Service instance: --
Link ID         : --
Nickname        : 0x0

IPv6 Address    : FE80::6A64:68FF:FE39:202
MAC address     : 6864-6839-0202          Type  : Dynamic
State           : STALE                   Aging : 126   seconds
Interface       : GE1/0/1                 VID   : 1
VPN instance    : --
Service instance: --
Link ID         : --
Nickname        : 0x0


IPv6 Address    : 1::4
MAC address     : 6864-6839-0204          Type  : Dynamic
State           : STALE                   Aging : 136   seconds
Interface       : GE1/0/2                  VID   : 1
VPN instance    : --
Service instance: 1
Link ID         : 0x1
Nickname        : 0x0
```

Table 9 Command output

Field	Description
IPv6 Address	IPv6 address of the neighbor.
MAC address	MAC address of the neighbor.
VID	ID of the VLAN to which the interface connected to a neighbor belongs. This field displays **N/A** if the VLAN ID is invalid.
Interface	Interface connected to a neighbor. If the interface name or link ID is not available, the field displays **N/A**. The link ID is a string with a maximum of eight hexadecimal numbers.
State	State of a neighbor:

Field	Description
	• **INCMP**—The address is being resolved. The link layer address of the neighbor is unknown. • **REACH**—The neighbor is reachable. • **STALE**—The reachability of the neighbor is unknown. The device will not verify the reachability unless it has data to send to the neighbor. • **DELAY**—The reachability of the neighbor is unknown. The device does not send an NS message in the delay period. • **PROBE**—The reachability of the neighbor is unknown. The device sends an NS message to probe the reachability of the neighbor.
Type	Neighbor information type: • **Static**—Statically configured. • **Dynamic**—Dynamically obtained. • **Openflow**—Learned from the OpenFlow module. • **Rule**—Learned from the portal module. • **Invalid static**—Invalid static configuration.
Aging	Reachable time of the neighbor: • For a static neighbor entry, this field displays hyphens (**--**), representing the neighbor entry never expires. • For a dynamic neighbor entry, this field displays the elapsed time in seconds. If the neighbor is never reachable, this field displays a pound sign (#).
VPN instance	This field is not supported in the current software version. Name of a VPN instance. This field displays hyphens (**--**) if no VPN instance is configured.
Service instance	This field is not supported in the current software version. Ethernet service instance. If the neighbor entry does not belong to any Ethernet service instance for the related Layer 2 Ethernet interface or Layer 2 aggregate interface, this field displays hyphens (**--**).
Link ID	This field is not supported in the current software version. ID of the link that connects to the neighbor. The link ID is a string with a maximum of eight hexadecimal numbers. If the neighbor entry does not belong to a VSI, the field displays hyphens (**--**).
Nickname	Nickname of a neighbor entry. The name is a string of four hexadecimal numbers.

Related commands

`ipv6 neighbor`

`reset ipv6 neighbors`

display ipv6 neighbors count

Use **`display ipv6 neighbors count`** to display the number of neighbor entries.

Syntax

`display ipv6 neighbors` { { **`all`** | **`dynamic`** | **`static`** } [**`slot`** *`slot-number`*] | **`interface`** *`interface-type interface-number`* | **`vlan`** *`vlan-id`* } **`count`**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

all: Displays the total number of all neighbor entries, including neighbor entries created dynamically and configured statically.

dynamic: Displays the total number of neighbor entries created dynamically.

static: Displays the total number of neighbor entries configured statically.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the number of neighbor entries for all member devices.

interface *interface-type interface-number*: Specifies an interface by its type and number.

vlan *vlan-id*: Displays the total number of neighbor entries in the specified VLAN. The value range for VLAN ID is 1 to 4094.

Examples

Display the total number of neighbor entries created dynamically.

```
<Sysname> display ipv6 neighbors dynamic count
 Total number of dynamic entries: 2
```

display ipv6 neighbors entry-limit

Use **display ipv6 neighbors entry-limit** to display the maximum number of ND entries that a device supports.

Syntax

display ipv6 neighbors entry-limit

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the maximum number of ND entries that the device supports.

```
<Sysname> display ipv6 neighbors entry-limit
ND entries: 256
```

display ipv6 pathmtu

Use the **display ipv6 pathmtu** command to display IPv6 Path MTU information.

Syntax

display ipv6 pathmtu { *ipv6-address* | { **all** | **dynamic** | **static** } [**count**] }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6-address: Specifies the destination IPv6 address for which the Path MTU information is to be displayed.

all: Displays all Path MTU information.

dynamic: Displays all dynamic Path MTU information.

static: Displays all static Path MTU information.

count: Displays the total number of Path MTU entries.

Examples

Display all Path MTU information.

```
<Sysname> display ipv6 pathmtu all
IPv6 destination address             PathMTU   Age   Type
1:2::3:2                             1800      -     Static
1:2::4:2                             1400      10    Dynamic
1:2::5:2                             1280      10    Dynamic
```

Displays the total number of Path MTU entries.

```
<Sysname> display ipv6 pathmtu all count
Total number of entries: 3
```

Table 10 Command output

Field	Description
PathMTU	Path MTU value on the network path to an IPv6 address.
Age	Time for a Path MTU to live. For a static Path MTU, this field displays a hyphen (-).
Type	Path MTU type: • **Dynamic**—Dynamically negotiated. • **Static**—Statically configured.
Total number of entries	Total number of Path MTU entries.

Related commands

ipv6 pathmtu

reset ipv6 pathmtu

display ipv6 prefix

Use **display ipv6 prefix** to display information about IPv6 prefixes, including dynamic and static prefixes.

Syntax

display ipv6 prefix [*prefix-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

prefix-number: Specifies the ID of an IPv6 prefix, in the range of 1 to 1024. If you do not specify an IPv6 prefix ID, this command displays information about all IPv6 prefixes.

Usage guidelines

A static IPv6 prefix is configured by using the **ipv6 prefix** command.

A dynamic IPv6 prefix is obtained from the DHCPv6 server, and its prefix ID is configured by using the **ipv6 dhcp client pd** command. For detailed information, see *Layer 3—IP Services Configuration Guide*.

Examples

Display information about all IPv6 prefixes.

```
<Sysname> display ipv6 prefix
Number  Prefix                                  Type
1       1::/16                                  Static
2       11:77::/32                              Dynamic
```

Display information about the IPv6 prefix with prefix ID 1.

```
<Sysname> display ipv6 prefix 1
Number: 1
Type  : Dynamic
Prefix: ABCD:77D8::/32
Preferred lifetime 90 sec, valid lifetime 120 sec
```

Table 11 Command output

Field	Description
Number	Prefix ID.
Type	Prefix type: • **Static**—Static IPv6 prefix. • **Dynamic**—Dynamic IPv6 prefix.
Prefix	Prefix and its length. If no prefix is obtained, this field displays **Not-available**.
Preferred lifetime 90 sec	Preferred lifetime in seconds. For a static IPv6 prefix, this field is not displayed.
valid lifetime 120 sec	Valid lifetime in seconds. For a static IPv6 prefix, this field is not displayed.

Related commands

ipv6 dhcp client pd

ipv6 prefix

display ipv6 rawip

Use **display ipv6 rawip** to display brief information about IPv6 RawIP connections.

Syntax

display ipv6 rawip [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays brief information about IPv6 RawIP connections for all member devices.

Examples

Display brief information about IPv6 RawIP connections.

```
<Sysname> display ipv6 rawip
Local Addr          Foreign Addr       Protocol Slot   PCB
2001:2002:2003:2    3001:3002:3003:3   58       1      0x0000000000000009
004:2005:2006:20    004:3005:3006:30
07:2008             07:3008
2002::100           2002::138          58       2      0x0000000000000008
::                  ::                 58       5      0x0000000000000002
```

Table 12 Command output

Field	Description
Local Addr	Local IPv6 address.
Foreign Addr	Peer IPv6 address.
Protocol	Protocol number.
PCB	PCB index.

display ipv6 rawip verbose

Use **display ipv6 rawip verbose** to display detailed information about IPv6 RawIP connections.

Syntax

display ipv6 rawip verbose [**slot** *slot-number* [**pcb** *pcb-index*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays detailed information about IPv6 RawIP connections for all member devices.

pcb *pcb-index*: Displays detailed information about IPv6 RawIP connections of the specified PCB. The value range for the *pcb-index* argument is 1 to 16.

Examples

Display detailed information about an IPv6 RawIP connection.

```
<Sysname> display ipv6 rawip verbose
Total RawIP socket number: 1

 Connection info: src = ::, dst = ::
 Location: slot: 6
 Creator: ping ipv6[320]
 State: N/A
 Options: N/A
 Error: 0
 Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 9216 / 1 / 0 / N/A
 Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A
 Type: 3
 Protocol: 58
 Inpcb flags: N/A
 Inpcb extflag: INP_EXTRCVICMPERR INP_EXTFILTER
 Inpcb vflag: INP_IPV6
 Hop limit: 255 (minimum hop limit: 0)
 Send VRF: 0xffff
 Receive VRF: 0xffff
```

Table 13 Command output

Field	Description
Total RawIP socket number	Total number of IPv6 RawIP sockets.
Connection info	Connection information, including the source and destination IPv6 addresses.
Location	Socket location.
Creator	Task name of the socket. The process number is in the square brackets.
State	Socket state: • **NOFDREF**—The user has closed the connection. • **ISCONNECTED**—The connection has been established. • **ISCONNECTING**—The connection is being established. • **ISDISCONNECTING**—The connection is being interrupted. • **ASYNC**—Asynchronous mode. • **ISDISCONNECTED**—The connection has been terminated. • **PROTOREF**—Indicates strong protocol reference. • **N/A**—None of above state.
Options	Socket options: • **SO_DEBUG**—Records socket debugging information. • **SO_ACCEPTCONN**—Enables the server to listen connection requests. • **SO_REUSEADDR**—Allows the local address reuse. • **SO_KEEPALIVE**—Requires the protocol to test whether the connection is still alive. • **SO_DONTROUTE**—Bypasses the routing table query for outgoing packets because the destination is in a directly connected network. • **SO_BROADCAST**—Supports broadcast packets. • **SO_LINGER**—Closes the socket. The system can still send remaining data in the socket send buffer. • **SO_OOBINLINE**—Stores the out-of-band data in the input queue.

Field	Description
	• **SO_REUSEPORT**—Allows the local port reuse. • **SO_TIMESTAMP**—Records the timestamps of the incoming packets, accurate to milliseconds. This option is applicable to protocols that are not connection orientated. • **SO_NOSIGPIPE**—Disables the socket from sending data. As a result, a sigpipe cannot be established when a return failure occurs. • **SO_TIMESTAMPNS**—Has a similar function with the timestamp, accurate to nanoseconds. • **SO_KEEPALIVETIME**—Sets a keepalive time. This option is supported in TCP. • **SO_FILTER**—Supports setting the packet filter criterion. This option is available for OSI Socket and RawIP. • **SO_USCBINDEX**—Obtains the user profile index from the received packets. • **N/A**—No options are set.
Error	Error code.

Receiving buffer (cc/hiwat/lowat/drop/state)	Displays receive buffer information in the following order:
	• **cc**—Used space.
	• **hiwat**—Maximum space.
	• **lowat**—Minimum space.
	• **drop**—Number of dropped packets.
	• **state**—Buffer state:
	  ○ **CANTSENDMORE**—Unable to send data to the peer.
	  ○ **CANTRCVMORE**—Unable to receive data from the peer.
	  ○ **RCVATMARK**—Receiving tag.
	  ○ **N/A**—None of the above states.

Sending buffer(cc/hiwat/lowat/state)	Displays send buffer information in the following order:
	• **cc**—Used space.
	• **hiwat**—Maximum space.
	• **lowat**—Minimum space.
	• **state**—Buffer state:
	  ○ **CANTSENDMORE**—Unable to send data to the peer.
	  ○ **CANTRCVMORE**—Unable to receive data from the peer.
	  ○ **RCVATMARK**—Receiving tag.
	  ○ **N/A**—None of the above states.

Type	Socket type: • **1**—**SOCK_STREAM**. This socket uses TCP to provide reliable transmission of byte streams. • **2**—**SOCK_DGRAM**. This socket uses UDP to provide datagram transmission. • **3**—**SOCK_RAW**. This socket allows an application to change the next upper-layer protocol header. • **N/A**—None of the above types.
Protocol	Number of protocol using the socket. 58 represents ICMP.
Inpcb flags	Flags in the Internet PCB: • **INP_RECVOPTS**—Receives IPv6 options. • **INP_RECVRETOPTS**—Receives replied IPv6 options. • **INP_RECVDSTADDR**—Receives destination IPv6 address. • **INP_HDRINCL**—Provides the entire IPv6 header. • **INP_REUSEADDR**—Reuses the IPv6 address. • **INP_REUSEPORT**—Reuses the port number.

Field	Description
	• **INP_ANONPORT**—Port number not specified. • **INP_PROTOCOL_PACKET**—Identifies a protocol packet. • **INP_RCVVLANID**—Receives the VLAN ID of the packet. Only UDP and RawIP support this flag. • **IN6P_IPV6_V6ONLY**—Only supports IPv6 protocol stack. • **IN6P_PKTINFO**—Receives the source IPv6 address and input interface of the packet. • **IN6P_HOPLIMIT**—Receives the hop limit. • **IN6P_HOPOPTS**—Receives the hop-by-hop options extension header. • **IN6P_DSTOPTS**—Receives the destination options extension header. • **IN6P_RTHDR**—Receives the routing extension header. • **IN6P_RTHDRDSTOPTS**—Receives the destination options extension header preceding the routing extension header. • **IN6P_TCLASS**—Receives the traffic class of the packet. • **IN6P_AUTOFLOWLABEL**—Attaches a flow label automatically. • **IN6P_RFC2292**—Uses the API specified in RFC 2292. • **IN6P_MTU**—Discovers differences in the MTU size of every link along a given data path. TCP does not support this flag. • **INP_RCVMACADDR**—Receives the MAC address of the frame. • **INP_USEICMPSRC**—Uses the specified IPv6 address as the source IPv6 address for outgoing ICMP packets. • **INP_SYNCPCB**—Waits until Internet PCB is synchronized. • **N/A**—None of the above flags.
Inpcb extflag	Extension flags in the Internet PCB: • **INP_EXTRCVPVCIDX**—Records the PVC index of the received packet. • **INP_RCVPWID**—Records the PW ID of the received packet. • **INP_EXTRCVICMPERR**—Receives an ICMP error packet. • **INP_EXTFILTER**—Filters the contents in the received packet. • **N/A**—None of the above flags.
Inpcb vflag	IP version flag in the Internet PCB: • **INP_IPV4**—IPv4 protocol. • **INP_IPV6**—IPv6 protocol. • **INP_IPV6PROTO**—Creates an Internet PCB based on IPv6 protocol. • **INP_TIMEWAIT**—In **TIMEWAIT** state. • **INP_ONESBCAST**—Sends broadcast packets. • **INP_DROPPED**—Protocol dropped flag. • **INP_SOCKREF**—Strong socket reference. • **INP_DONTBLOCK**—Do not block synchronization of the Internet PCB. • **N/A**—None of the above flags.
Hop limit	Hop limit in the Internet PCB.
Send VRF	This field is not supported in the current software version. VRF from which packets are sent.
Receive VRF	This field is not supported in the current software version. VRF from which packets are received.

display ipv6 statistics

Use **display ipv6 statistics** to display IPv6 and ICMPv6 packet statistics.

Syntax

display ipv6 statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 and ICMPv6 packet statistics for all member devices.

Examples

Display IPv6 and ICMPv6 packet statistics.

```
<Sysname> display ipv6 statistics
  IPv6 statistics:

    Sent packets:
      Total:     0
        Sent locally:        0          Forwarded:            0
        Raw packets:         0          Discarded:            0
        Fragments:           0          Fragments failed:     0
        Routing failed:      0

    Received packets:
      Total:     0
        Received locally:    0          Hop limit exceeded:  0
        Fragments:           0          Reassembled:          0
        Reassembly failures:  0          Reassembly timeout:  0
        Format errors:       0          Option errors:       0
        Protocol errors:     0

  ICMPv6 statistics:

    Sent packets:
      Total:     0
        Unreachable:         0           Too big:             0
        Hop limit exceeded:  0           Reassembly timeouts: 0
        Parameter problems:  0
        Echo requests:       0           Echo replies:        0
        Neighbor solicits:   0           Neighbor adverts:    0
        Router solicits:     0           Router adverts:      0
        Redirects:           0           Router renumbering:  0
      Send failed:
```

```
    Rate limitation:     0          Other errors:        0

  Received packets:
   Total:     0
     Checksum errors:     0          Too short:           0
     Bad codes:           0
     Unreachable:         0          Too big:             0
     Hop limit exceeded:  0          Reassembly timeouts:  0
     Parameter problems:  0          Unknown error types:  0
     Echo requests:       0          Echo replies:        0
     Neighbor solicits:   0          Neighbor adverts:    0
     Router solicits:     0          Router adverts:      0
     Redirects:           0          Router renumbering:  0
     Unknown info types:  0
   Deliver failed:
     Bad length:         0
```

Related commands

reset ipv6 statistics

display ipv6 tcp

Use **display ipv6 tcp** to display brief information about IPv6 TCP connections.

Syntax

display ipv6 tcp [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays brief information about IPv6 TCP connections for all member devices.

Examples

Display brief information about IPv6 TCP connections.

```
<Sysname> display ipv6 tcp
*: TCP connection with authentication
 LAddr->port        FAddr->port      State       Slot   PCB
*2001:2002:2003:2   3001:3002:3003:3 ESTABLISHED 1     0x000000000000c387
004:2005:2006:20    004:3005:3006:30
07:2008->1200       07:3008->1200
2001::1->23         2001::5->1284    ESTABLISHED 2     0x0000000000000008
2003::1->25         2001::2->1283    LISTEN      3     0x0000000000000009
```

Table 14 Command output

Field	Description
*	Indicates that the TCP connection uses authentication.
LAddr->port	Local IPv6 address and port number.
FAddr->port	Peer IPv6 address and port number.
State	IPv6 TCP connection state.
PCB	PCB index.

display ipv6 tcp verbose

Use **display ipv6 tcp verbose** to display detailed information about IPv6 TCP connections.

Syntax

display ipv6 tcp verbose [**slot** *slot-number* [**pcb** *pcb-index*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays detailed information about IPv6 TCP connections for all member devices.

pcb *pcb-index*: Displays detailed information about IPv6 TCP connections of the specified PCB. The value range for the *pcb-index* argument is 1 to 16.

Examples

Display detailed information about an IPv6 TCP connection.

```
<Sysname> display ipv6 tcp verbose
TCP inpcb number: 1(tcpcb number: 1)

 Connection info: src = 2001::1->179 ,  dst = 2001::2->4181
 Location: Slot: 6
 NSR standby: N/A
 Creator: bgpd[199]
 State: ISCONNECTED
 Options: N/A
 Error: 0
 Receiving buffer(cc/hiwat/lowat/state): 0 / 65536 / 1 / N/A
 Sending buffer(cc/hiwat/lowat/state): 0 / 65536 / 512 / N/A
 Type: 1
 Protocol: 6
 Inpcb flags: N/A
 Inpcb extflag: N/A
 Inpcb vflag: INP_IPV6
```

```
Hop limit: 255 (minimum hop limit: 0)
Connection state: ESTABLISHED
TCP options: TF_REQ_SCALE TF_REQ_TSTMP TF_SACK_PERMIT TF_NSR
NSR state: READY(M)
Send VRF: 0x0
Receive VRF: 0x0
```

Table 15 Command output

Field	Description
TCP inpcb number	Number of IPv6 TCP Internet PCBs.
Connection info	Connection information, including source IPv6 address, source port number, destination IPv6 address, and destination port number.
Location	Socket location.
tcpcb number	Number of IPv6 TCP PCBs (excluding PCBs of TCP in TIME_WAIT state).
Creator	Task name of the socket. The process number is in the square brackets.
State	Socket state: • **NOFDREF**—The user has closed the connection. • **ISCONNECTED**—The connection has been established. • **ISCONNECTING**—The connection is being established. • **ISDISCONNECTING**—The connection is being interrupted. • **ASYNC**—Asynchronous mode. • **ISDISCONNECTED**—The connection has been terminated. • **PROTOREF**—Indicates strong protocol reference. • **N/A**—None of above state.
Options	Socket options: • **SO_DEBUG**—Records socket debugging information. • **SO_ACCEPTCONN**—Enables the server to listen connection requests. • **SO_REUSEADDR**—Allows the local address reuse. • **SO_KEEPALIVE**—Requires the protocol to test whether the connection is still alive. • **SO_DONTROUTE**—Bypasses the routing table query for outgoing packets because the destination is in a directly connected network. • **SO_BROADCAST**—Supports broadcast packets. • **SO_LINGER**—Closes the socket. The system can still send remaining data in the socket send buffer. • **SO_OOBINLINE**—Stores the out-of-band data in the input queue. • **SO_REUSEPORT**—Allows the local port reuse. • **SO_NOSIGPIPE**—Disables the socket from sending data. As a result, a sigpipe cannot be established when a return failure occurs. • **SO_TIMESTAMPNS**—Has a similar function with the timestamp, accurate to nanoseconds. • **SO_KEEPALIVETIME**—Sets a keepalive time. This option is supported in TCP. • **SO_FILTER**—Supports setting the packet filter criterion. This option is available for OSI Socket and RawIP. • **N/A**—No options are set.
Error	Error code.
Receiving buffer(cc/hiwat/lowat/state)	Displays receive buffer information in the following order: • **cc**—Used space.

Field	Description

	• **hiwat**—Maximum space.
	• **lowat**—Minimum space.
	• **state**—Buffer state:
	  ○ **CANTSENDMORE**—Unable to send data to the peer.
	  ○ **CANTRCVMORE**—Unable to receive data from the peer.
	  ○ **RCVATMARK**—Receiving tag.
	  ○ **N/A**—None of the above states.

Sending buffer(cc/hiwat/lowat/state)	Displays send buffer information in the following order:
	• **cc**—Used space.
	• **hiwat**—Maximum space.
	• **lowat**—Minimum space.
	• **state**—Buffer state:
	  ○ **CANTSENDMORE**—Unable to send data to the peer.
	  ○ **CANTRCVMORE**—Unable to receive data from the peer.
	  ○ **RCVATMARK**—Receiving tag.
	  ○ **N/A**—None of the above states.

Type	Socket type: • **1**—**SOCK_STREAM**. This socket uses TCP to provide reliable transmission of byte streams. • **2**—**SOCK_DGRAM**. This socket uses UDP to provide datagram transmission. • **3**—**SOCK_RAW**. This socket allows an application to change the next upper-layer protocol header. • **N/A**—None of the above types.
Protocol	Number of the protocol using the socket. 6 represents TCP.
Inpcb flags	Flags in the Internet PCB: • **INP_RECVOPTS**—Receives IPv6 options. • **INP_RECVRETOPTS**—Receives replied IPv6 options. • **INP_RECVDSTADDR**—Receives destination IPv6 address. • **INP_HDRINCL**—Provides the entire IPv6 header. • **INP_REUSEADDR**—Reuses the IPv6 address. • **INP_REUSEPORT**—Reuses the port number. • **INP_ANONPORT**—Port number not specified. • **INP_PROTOCOL_PACKET**—Identifies a protocol packet. • **INP_RCVVLANID**—Receives the VLAN ID of the packet. Only UDP and RawIP support this flag. • **IN6P_IPV6_V6ONLY**—Only supports IPv6 protocol stack. • **IN6P_PKTINFO**—Receives the source IPv6 address and input interface of the packet. • **IN6P_HOPLIMIT**—Receives the hop limit. • **IN6P_HOPOPTS**—Receives the hop-by-hop options extension header. • **IN6P_DSTOPTS**—Receives the destination options extension header. • **IN6P_RTHDR**—Receives the routing extension header. • **IN6P_RTHDRDSTOPTS**—Receives the destination options extension header preceding the routing extension header. • **IN6P_TCLASS**—Receives the traffic class of the packet. • **IN6P_AUTOFLOWLABEL**—Attaches a flow label automatically. • **IN6P_RFC2292**—Uses the API specified in RFC 2292. • **IN6P_MTU**—Discovers differences in the MTU size of every link along a given data path. TCP does not support this flag.

Field	Description
	• **INP_RCVMACADDR**—Receives the MAC address of the frame. • **INP_SYNCPCB**—Waits until Internet PCB is synchronized. • **N/A**—None of the above flags.
Inpcb extflag	Extension flags in the Internet PCB: • **INP_EXTRCVPVCIDX**—Records the PVC index of the received packet. • **INP_RCVPWID**—Records the PW ID of the received packet. • **INP_EXTDONTDROP**—Does not drop the received packet. • **INP_EXLISTEN**—Listening socket. • **N/A**—None of the above flags.
Inpcb vflag	IP version flags in the Internet PCB: • **INP_IPV4**—IPv4 protocol. • **INP_IPV6**—IPv6 protocol. • **INP_IPV6PROTO**—Creates an Internet PCB based on IPv6 protocol. • **INP_TIMEWAIT**—In **TIMEWAIT** state. • **INP_ONESBCAST**—Sends broadcast packets. • **INP_DROPPED**—Protocol dropped flag. • **INP_SOCKREF**—Strong socket reference. • **INP_DONTBLOCK**—Do not block synchronization of the Internet PCB. • **N/A**—None of the above flags.
Hop limit	Hop limit in the Internet PCB.
Connection state	TCP connection state: • **CLOSED**—The server receives a disconnection request's reply from the client. • **LISTEN**—The server is waiting for connection requests. • **SYN_SENT**—The client is waiting for the server to reply to the connection request. • **SYN_RCVD**—The server receives a connection request. • **ESTABLISHED**—The server and client have established connections and can transmit data bidirectionally. • **CLOSE_WAIT**—The server receives a disconnection request from the client. • **FIN_WAIT_1**—The client is waiting for the server to reply to a disconnection request. • **CLOSING**—The server and client are waiting for peer's disconnection reply when receiving disconnection requests from each other. • **LAST_ACK**—The server is waiting for the client to reply to a disconnection request. • **FIN_WAIT_2**—The client receives a disconnection reply from the server. • **TIME_WAIT**—The client receives a disconnection request from the server.
TCP options	TCP options: • **TF_MD5SIG**—Enables MD5 signature. • **TF_NODELAY**—Disables the Nagle algorithm that buffers the sent data inside the TCP. • **TF_NOOPT**—No TCP options. • **TF_NOPUSH**—Forces TCP to delay sending any TCP data until a full sized segment is buffered in the TCP buffers. • **TF_BINDFOREIGNADDR**—Binds the peer IP address.

Field	Description
	• **TF_NSR**—Enables TCP NSR. • **TF_REQ_SCALE**—Enables the TCP window scale option. • **TF_REQ_TSTMP**—Enables the time stamp option. • **TF_SACK_PERMIT**—Enables the TCP selective acknowledgement option. • **TF_ENHANCED_AUTH**—Enables the enhanced authentication option.
NSR state	State of the TCP connections. Between the parentheses is the role of the connection: • **M**—Main connection. • **S**—Standby connection.
Send VRF	This field is not supported in the current software version. VRF from which packets are sent.
Receive VRF	This field is not supported in the current software version. VRF from which packets are received.

display ipv6 udp

Use **display ipv6 udp** to display brief information about IPv6 UDP connections.

Syntax

display ipv6 udp [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays brief information about IPv6 UDP connections for all member devices.

Examples

Displays brief information about IPv6 UDP connections.

```
<Sysname> display ipv6 udp
 LAddr->port        FAddr->port        Slot  PCB
 2001:2002:2003:2   3001:3002:3003:3   1     0x000000000000c387
 004:2005:2006:20   004:3005:3006:30
 07:2008->1200      07:3008->1200
 2001::1->23        2001::5->1284      2     0x0000000000000008
 2003::1->25        2001::2->1283      3     0x0000000000000009
```

Table 16 Command output

Field	Description
LAddr->port	Local IPv6 address and port number.

Field	Description
FAddr->port	Peer IPv6 address and port number.
PCB	PCB index.

display ipv6 udp verbose

Use **display ipv6 udp verbose** to display detailed information about IPv6 UDP connections.

Syntax

display ipv6 udp verbose [**slot** *slot-number* [**pcb** *pcb-index*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays detailed information about IPv6 UDP connections for all member devices.

pcb *pcb-index*: Displays detailed information about IPv6 UDP connections of the specified PCB. The value range for the *pcb-index* argument is 1 to 16.

Examples

Display detailed information about an IPv6 UDP connection.

```
<Sysname> display ipv6 udp verbose
Total UDP socket number: 1

 Connection info: src = ::->69, dst = ::->0
 Location: slot: 6
 Creator: sock_test_mips[250]
 State: N/A
 Options: N/A
 Error: 0
 Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 41600 / 1 / 0 / N/A
 Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A
 Type: 2
 Protocol: 17
 Inpcb flags: N/A
 Inpcb extflag: N/A
 Inpcb vflag: INP_IPV6
 Hop limit: 255 (minimum hop limit: 0)
 Send VRF: 0xffff
 Receive VRF: 0xffff
```

Table 17 Command output

Field	Description
Total UDP socket number	Total number of IPv6 UDP sockets.
Connection info	Connection information, including source IPv6 address, source port number, destination IPv6 address, and destination port number.
Location	Socket location.
Creator	Task name of the socket. The progress number is in the square brackets.
State	Socket state: • **NOFDREF**—The user has closed the connection. • **ISCONNECTED**—The connection has been established. • **ISCONNECTING**—The connection is being established. • **ISDISCONNECTING**—The connection is being interrupted. • **ASYNC**—Asynchronous mode. • **ISDISCONNECTED**—The connection has been terminated. • **PROTOREF**—Indicates strong protocol reference. • **N/A**—None of above state.
Options	Socket options: • **SO_DEBUG**—Records socket debugging information. • **SO_ACCEPTCONN**—Enables the server to listen connection requests. • **SO_REUSEADDR**—Allows the local address reuse. • **SO_KEEPALIVE**—Requires the protocol to test whether the connection is still alive. • **SO_DONTROUTE**—Bypasses the routing table query for outgoing packets because the destination is in a directly connected network. • **SO_BROADCAST**—Supports broadcast packets. • **SO_LINGER**—Closes the socket. The system can still send remaining data in the socket send buffer. • **SO_OOBINLINE**—Stores the out-o-band data in the input queue. • **SO_REUSEPORT**—Allows the local port reuse. • **SO_TIMESTAMP**—Records the timestamps of the input packets, accurate to milliseconds. This option is applicable to protocols that are not connection orientated. • **SO_NOSIGPIPE**—Disables the socket from sending data. As a result, a sigpipe cannot be established when a return failure occurs. • **SO_TIMESTAMPNS**—Has a similar function with the timestamp, accurate to nanoseconds. • **SO_KEEPALIVETIME**—Sets a keepalive time. This option is supported in TCP. • **SO_FILTER**—Supports setting the packet filter criterion. This option is available for OSI Socket and RawIP. • **SO_USCBINDEX**—Obtains the user profile index from the received packets. • **N/A**—No options are set.
Error	Error code.
Receiving buffer(cc/hiwat/lowat/drop/state)	Displays receive buffer information in the following order: • **cc**—Used space. • **hiwat**—Maximum space. • **lowat**—Minimum space. • **drop**—Number of dropped packets.

Field	Description

	• **state**—Buffer state:
	  ○ **CANTSENDMORE**—Unable to send data to the peer.
	  ○ **CANTRCVMORE**—Unable to receive data from the peer.
	  ○ **RCVATMARK**—Receiving tag.
	  ○ **N/A**—None of the above states.

Sending buffer(cc/hiwat/lowat/state)	Displays send buffer information in the following order:
	• **cc**—Used space.
	• **hiwat**—Maximum space.
	• **lowat**—Minimum space.
	• **state**—Buffer state:
	  ○ **CANTSENDMORE**—Unable to send data to the peer.
	  ○ **CANTRCVMORE**—Unable to receive data from the peer.
	  ○ **RCVATMARK**—Receiving tag.
	  ○ **N/A**—None of the above states.

Type	Socket type: • **1**—**SOCK_STREAM**. This socket uses TCP to provide reliable transmission of byte streams. • **2**—**SOCK_DGRAM**. This socket uses UDP to provide datagram transmission. • **3**—**SOCK_RAW**. This socket allows an application to change the next upper-layer protocol header. • **N/A**—None of the above types.
Protocol	Number of the protocol using the socket. 17 represents UDP.
Inpcb flags	Flags in the Internet PCB: • **INP_RECVOPTS**—Receives IPv6 options. • **INP_RECVRETOPTS**—Receives replied IPv6 options. • **INP_RECVDSTADDR**—Receives destination IPv6 address. • **INP_HDRINCL**—Provides the entire IPv6 header. • **INP_REUSEADDR**—Reuses the IPv6 address. • **INP_REUSEPORT**—Reuses the port number. • **INP_ANONPORT**—Port number not specified. • **INP_PROTOCOL_PACKET**—Identifies a protocol packet. • **INP_RCVVLANID**—Receives the VLAN ID of the packet. Only UDP and RawIP support this flag. • **IN6P_IPV6_V6ONLY**—Only supports IPv6 protocol stack. • **IN6P_PKTINFO**—Receives the source IPv6 address and input interface of the packet. • **IN6P_HOPLIMIT**—Receives the hop limit. • **IN6P_HOPOPTS**—Receives the hop-by-hop options extension header. • **IN6P_DSTOPTS**—Receives the destination options extension header. • **IN6P_RTHDR**—Receives the routing extension header. • **IN6P_RTHDRDSTOPTS**—Receives the destination options extension header preceding the routing extension header. • **IN6P_TCLASS**—Receives the traffic class of the packet. • **IN6P_AUTOFLOWLABEL**—Attaches a flow label automatically. • **IN6P_RFC2292**—Uses the API specified in RFC 2292. • **IN6P_MTU**—Discovers differences in the MTU size of every link along a given data path. TCP does not support this flag. • **INP_RCVMACADDR**—Receives the MAC address of the frame.

Field	Description
	• **INP_SYNCPCB**—Waits until Internet PCB is synchronized. • **N/A**—None of the above flags.
Inpcb extflag	Extension flags in the Internet PCB: • **INP_EXTRCVPVCIDX**—Records the PVC index of the received packet. • **INP_RCVPWID**—Records the PW ID of the received packet. • **N/A**—None of the above flags.
Inpcb vflag	IP version flags in the Internet PCB: • **INP_IPV4**—IPv4 protocol. • **INP_IPV6**—IPv6 protocol. • **INP_IPV6PROTO**—Creates an Internet PCB based on IPv6 protocol. • **INP_TIMEWAIT**—In **TIMEWAIT** state. • **INP_ONESBCAST**—Sends broadcast packets. • **INP_DROPPED**—Protocol dropped flag. • **INP_SOCKREF**—Strong socket reference. • **INP_DONTBLOCK**—Do not block synchronization of the Internet PCB. • **N/A**—None of the above flags.
Hop limit	Hop limit in the Internet PCB.
Send VRF	This field is not supported in the current software version. VRF from which packets are sent.
Receive VRF	This field is not supported in the current software version. VRF from which packets are received.

ipv6 address

Use **ipv6 address** to configure an IPv6 global unicast address for an interface.

Use **undo ipv6 address** to delete an IPv6 global unicast address of the interface.

Syntax

ipv6 address { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* }

undo ipv6 address [*ipv6-address prefix-length* | *ipv6-address*/*prefix-length*]

Default

No IPv6 global unicast address is configured for an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies an IPv6 address.

prefix-length: Specifies a prefix length in the range of 1 to 128.

Usage guidelines

Like public IPv4 addresses, IPv6 global unicast addresses are assigned to ISPs. This type of address allows for prefix aggregation to reduce the number of global routing entries.

If you do not specify any parameters, the **undo ipv6 address** command deletes all IPv6 addresses of an interface.

Examples

Set the IPv6 global unicast address of VLAN-interface 100 to 2001::1 with prefix length 64.

Method 1:

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1/64
```

Method 2:

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1 64
```

ipv6 address anycast

Use **ipv6 address anycast** to configure an IPv6 anycast address for an interface.

Use **undo ipv6 address anycast** to delete the IPv6 anycast address of the interface.

Syntax

ipv6 address { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* } **anycast**

undo ipv6 address { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* } **anycast**

Default

No IPv6 anycast address is configured for an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies an IPv6 anycast address.

prefix-length: Specifies a prefix length in the range of 1 to 128.

Examples

Set the IPv6 anycast address of VLAN-interface 100 to 2001::1 with prefix length 64.

Method 1:

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1/64 anycast
```

Method 2:

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
```

```
[Sysname-Vlan-interface100] ipv6 address 2001::1 64 anycast
```

ipv6 address auto

Use **ipv6 address auto** to enable the stateless address autoconfiguration feature on an interface, so that the interface can automatically generate a global unicast address.

Use **undo ipv6 address auto** to disable this feature.

Syntax

ipv6 address auto

undo ipv6 address auto

Default

The stateless address autoconfiguration feature is disabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

After a global unicast address is generated through stateless autoconfiguration, a link-local address is generated automatically.

To delete the global unicast address and the link-local address that are automatically generated, use either of the following commands:

- **undo ipv6 address auto**
- **undo ipv6 address**

Examples

Enable stateless address autoconfiguration on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address auto
```

ipv6 address auto link-local

Use **ipv6 address auto link-local** to automatically generate a link-local address for an interface.

Use **undo ipv6 address auto link-local** to restore the default.

Syntax

ipv6 address auto link-local

undo ipv6 address auto link-local

Default

No link-local address is configured on an interface. A link-local address is automatically generated after an IPv6 global unicast address is configured for the interface.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

Link-local addresses are used for neighbor discovery and stateless autoconfiguration on the local link. Packets using link-local addresses as the source or destination addresses cannot be forwarded to other links.

After an IPv6 global unicast address is configured for an interface, a link-local address is automatically generated. This link-local address is the same as the one generated by using the **ipv6 address auto link-local** command.

The **undo ipv6 address auto link-local** command deletes only the link-local addresses generated through the **ipv6 address auto link-local** command. If the **undo** command is executed on an interface with an IPv6 global unicast address configured, the interface still has a link-local address.

You can also manually assign an IPv6 link-local address for an interface by using the **ipv6 address link-local** command. Manual assignment takes precedence over automatic generation for IPv6 link-local addresses.

- If you first use automatic generation and then manual assignment, the manually assigned link-local address overwrites the automatically generated address.
- If you first use manual assignment and then automatic generation, both of the following occur:
  - The automatically generated link-local address does not take effect.
  - The link-local address of an interface is still the manually assigned address.

  If you delete the manually assigned address, the automatically generated link-local address takes effect.

Examples

Configure VLAN-interface 100 to automatically generate a link-local address.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address auto link-local
```

Related commands

ipv6 address link-local

ipv6 address eui-64

Use **ipv6 address eui-64** to configure an EUI-64 IPv6 address for an interface.

Use **undo ipv6 address eui-64** to delete an EUI-64 IPv6 address from an interface.

Syntax

ipv6 address { *ipv6-address prefix-length* | *ipv6-address/prefix-length* } **eui-64**

undo ipv6 address { *ipv6-address prefix-length* | *ipv6-address/prefix-length* } **eui-64**

Default

No EUI-64 IPv6 address is configured for an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-address prefix-length: Specifies an IPv6 address and IPv6 prefix length. The *ipv6-address* and *prefix-length* arguments jointly specify the prefix of an EUI-64 IPv6 address. The value range for the *prefix-length* argument is 1 to 64. The IPv6 address and IPv6 prefix length support the following formats:

- *ipv6-address/prefix-length*. For example: 2001::1/64.
- *ipv6-address prefix-length*. For example: 2001::1 64.

Usage guidelines

An EUI-64 IPv6 address is generated based on the specified prefix and the automatically generated interface ID. To display the EUI-64 IPv6 address, use the **display ipv6 interface** command.

The prefix length of an EUI-64 IPv6 address cannot be greater than 64.

Examples

Configure an EUI-64 IPv6 address for VLAN-interface 100. The prefix of the address is the same as that of 2001::1/64, and the interface ID is generated based on the MAC address of the device.

Method 1:

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1/64 eui-64
```

Method 2:

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1 64 eui-64
```

Related commands

display ipv6 interface

ipv6 address link-local

Use **ipv6 address link-local** to configure a link-local address for the interface.

Use **undo ipv6 address link-local** to restore the default.

Syntax

ipv6 address { *ipv6-address* [*prefix-length*] | *ipv6-address/prefix-length* } **link-local**

undo ipv6 address { *ipv6-address* [*prefix-length*] | *ipv6-address/prefix-length* } **link-local**

Default

No link-local address is configured for the interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies an IPv6 link-local address. The first 10 bits of an address must be 1111111010 (binary). The first group of hexadecimals in the address must be FE80 to FEBF.

prefix-length: Specifies an IPv6 prefix length, in the range of 1 to 128.

Usage guidelines

Manual assignment takes precedence over automatic generation.

If you use automatic generation, and then use manual assignment, the manually assigned link-local address overwrites the one that is automatically generated.

If you use manual assignment and then use automatic generation, both of the following occur:

- The automatically generated link-local address does not take effect.
- The manually assigned link-local address of an interface remains.

After you delete the manually assigned address, the automatically generated link-local address takes effect. For automatic generation of an IPv6 link-local address, see the **ipv6 address auto link-local** command.

When you configure a link-local address, make sure the prefix length is equal to or greater than 10. Otherwise, the configuration fails.

Examples

Configure a link-local address for VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address fe80::1 link-local
```

Configure a link-local address for VLAN-interface 100 and set the prefix length to 64.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address fe80::1 64 link-local
```

Related commands

ipv6 address auto link-local

ipv6 address *prefix-number*

Use **ipv6 address** *prefix-number* to specify an IPv6 prefix for an interface to automatically generate an IPv6 global unicast address and advertise the prefix.

Use **undo ipv6 address** *prefix-number* to restore the default.

Syntax

ipv6 address *prefix-number sub-prefix/prefix-length*

undo ipv6 address *prefix-number*

Default

No IPv6 prefix is specified for IPv6 address autoconfiguration.

Views

Interface view

Predefined user roles

network-admin

Parameters

prefix-number: Specifies an IPv6 prefix by its ID in the range of 1 to 1024. The specified IPv6 prefix can be manually configured or obtained through DHCPv6.

sub-prefix: Specifies the sub-prefix bit and host bit for the IPv6 global unicast address.

prefix-length: Specifies the sub-prefix length in the range of 1 to 128.

Usage guidelines

This command enables an interface to automatically generate an IPv6 global unicast address based on the specified IPv6 prefix, sub-prefix bit, and host bit.

An interface can generate only one IPv6 global unicast address based on the prefix specified by using the **ipv6 address** command. To configure the interface to generate a new IPv6 address, execute the **undo ipv6 address** command to delete the configuration, and then execute the **ipv6 address** command.

Examples

Configure a static IPv6 prefix AAAA::/16 and assign ID 1 to the prefix. Configure VLAN-interface 100 to use this prefix to generate the IPv6 address AAAA:CCCC:DDDD::10/32 and advertise this prefix.

```
<Sysname> system-view
[Sysname] ipv6 prefix 1 AAAA::/16
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 1 BBBB:CCCC:DDDD::10/32
```

Configure VLAN-interface 10 to obtain an IPv6 prefix through DHCPv6 and assign ID 2 to the obtained prefix. Configure VLAN-interface 100 to use the obtained prefix to generate the IPv6 address AAAA:CCCC:DDDD::10/32 and advertise the prefix.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ipv6 dhcp client pd 2 rapid-commit option-group 1
[Sysname-Vlan-interface10] quit
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2 BBBB:CCCC:DDDD::10/32
```

Related commands

ipv6 prefix

ipv6 dhcp client pd

ipv6 hop-limit

Use **ipv6 hop-limit** to set the Hop Limit field in the IPv6 header.

Use **undo ipv6 hop-limit** to restore the default.

Syntax

ipv6 hop-limit *value*

undo ipv6 hop-limit

Default

The hop limit is 64.

Views

System view

Predefined user roles

network-admin

Parameters

value: Specifies the number of hops, in the range of 1 to 255.

Usage guidelines

The hop limit determines the number of hops that an IPv6 packet generated by the device can travel.

The device advertises the hop limit in RA messages. All RA message receivers use the advertised value to fill in the Hop Limit field for IPv6 packets to be sent. To disable the device from advertising the hop limit, use the **ipv6 nd ra hop-limit unspecified** command.

Examples

Set the maximum number of hops to 100.

```
<Sysname> system-view
[Sysname] ipv6 hop-limit 100
```

Related commands

ipv6 nd ra hop-limit unspecified

ipv6 hoplimit-expires enable

Use **ipv6 hoplimit-expires enable** to enable sending ICMPv6 time exceeded messages.

Use **undo ipv6 hoplimit-expires** to disable sending ICMPv6 time exceeded messages.

Syntax

ipv6 hoplimit-expires enable

undo ipv6 hoplimit-expires enable

Default

Sending ICMPv6 time exceeded messages is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

ICMPv6 time exceeded messages are sent to the source of IPv6 packets after the device discards IPv6 packets because hop or reassembly times out.

To prevent too many ICMPv6 error messages from affecting device performance, disable this feature. Even with the feature disabled, the device still sends fragment reassembly time exceeded messages.

Examples

Disable sending ICMPv6 time exceeded messages.

```
<Sysname> system-view
[Sysname] undo ipv6 hoplimit-expires enable
```

ipv6 icmpv6 error-interval

Use **ipv6 icmpv6 error-interval** to set the bucket size and the interval for tokens to arrive in the bucket for ICMPv6 error messages.

Use **undo ipv6 icmpv6 error-interval** to restore the default.

Syntax

ipv6 icmpv6 error-interval *interval* [*bucketsize*]

undo ipv6 icmpv6 error-interval

Default

The bucket allows a maximum of 10 tokens, and a token is placed in the bucket every 100 milliseconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the interval for tokens to arrive in the bucket. The value range is 0 to 2147483647 milliseconds. To disable the ICMPv6 rate limit, set the value to 0.

bucketsize: Specifies the maximum number of tokens allowed in the bucket. The value range is 1 to 200.

Usage guidelines

This command limits the rate at which ICMPv6 error messages are sent. Use this command to prevent network congestion caused by excessive ICMPv6 error messages generated within a short period. A token bucket algorithm is used with one token representing one ICMPv6 error message.

A token is placed in the bucket at intervals until the maximum number of tokens that the bucket can hold is reached.

A token is removed from the bucket when an ICMPv6 error message is sent. When the bucket is empty, ICMPv6 error messages are not sent until a new token is placed in the bucket.

Examples

Set the bucket size to 40 tokens and the interval for tokens to arrive in the bucket to 200 milliseconds for ICMPv6 error messages.

```
<Sysname> system-view
[Sysname] ipv6 icmpv6 error-interval 200 40
```

ipv6 icmpv6 multicast-echo-reply enable

Use **ipv6 icmpv6 multicast-echo-reply enable** to enable replying to multicast echo requests.

Use **undo ipv6 icmpv6 multicast-echo-reply** to restore the default.

Syntax

ipv6 icmpv6 multicast-echo-reply enable

undo ipv6 icmpv6 multicast-echo-reply enable

Default

The device is disabled from replying to multicast echo requests.

Views

System view

Predefined user roles

network-admin

Usage guidelines

If a host is configured to reply to multicast echo requests, an attacker can use this mechanism to attack the host. For example, the attacker can send an echo request to a multicast address with Host A as the source. All hosts in the multicast group will send echo replies to Host A.

To prevent attacks, do not enable the device to reply to multicast echo requests unless necessary.

Examples

Enable replying to multicast echo requests.

```
<Sysname> system-view
[Sysname] ipv6 icmpv6 multicast-echo-reply enable
```

ipv6 icmpv6 source

Use **ipv6 icmpv6 source** to specify a source IPv6 address for unsolicited ICMPv6 packets.

Use **undo ipv6 icmpv6 source** to restore the default.

Syntax

ipv6 icmpv6 source *ipv6-address*

undo ipv6 icmpv6 source

Default

No IPv6 source address is specified for unsolicited ICMPv6 packets.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies an IPv6 address.

Usage guidelines

For ICMPv6 echo requests, the source IPv6 address specified in the **ping ipv6** command has higher priority than the source IPv6 address specified in this command.

Examples

Specify IPv6 address 1::1 as the source address for unsolicited ICMPv6 packets.

```
<Sysname> system-view
[Sysname] ipv6 icmpv6 source 1::1
```

ipv6 mtu

Use **ipv6 mtu** to set the interface MTU for IPv6 packets.

Use **undo ipv6 mtu** to restore the default.

Syntax

ipv6 mtu *size*

undo ipv6 mtu

Default

The interface MTU is not configured.

Views

Interface view

Predefined user roles

network-admin

Parameters

size: Specifies the MTU size in bytes. The value range for this argument is 1280 to 1500.

Usage guidelines

If the size of a packet exceeds the MTU of the sending interface, the device discards the packet. If the device is an intermediate device, it also sends the source host an ICMPv6 Packet Too Big message with the MTU of the sending interface. The source host fragments the packets according to the MTU. To avoid this situation, set a proper interface MTU.

Examples

Set the interface MTU for IPv6 packets to 1280 bytes on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 mtu 1280
```

ipv6 nd autoconfig managed-address-flag

Use **ipv6 nd autoconfig managed-address-flag** to set the managed address configuration flag (M) to 1 in RA advertisements to be sent.

Use **undo ipv6 nd autoconfig managed-address-flag** to restore the default.

Syntax

ipv6 nd autoconfig managed-address-flag

undo ipv6 nd autoconfig managed-address-flag

Default

The M flag is set to **0** in RA advertisements. Hosts receiving the advertisements will obtain IPv6 addresses through stateless autoconfiguration.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

The M flag in RA advertisements determines whether receiving hosts use stateful autoconfiguration to obtain IPv6 addresses.

- If the M flag is set to 1 in RA advertisements, receiving hosts use stateful autoconfiguration (for example, from an DHCPv6 server) to obtain IPv6 addresses.
- If the M flag is set to 0 in RA advertisements, receiving hosts use stateless autoconfiguration. Stateless autoconfiguration generates IPv6 addresses according to link-layer addresses and the prefix information in the RA advertisements.

Examples

Set the M flag to 1 in RA advertisements to be sent.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd autoconfig managed-address-flag
```

ipv6 nd autoconfig other-flag

Use **ipv6 nd autoconfig other-flag** to set the other stateful configuration flag (O) to 1 in RA advertisements to be sent.

Use **undo ipv6 nd autoconfig other-flag** to restore the default.

Syntax

ipv6 nd autoconfig other-flag

undo ipv6 nd autoconfig other-flag

Default

The O flag is set to **0** in RA advertisements. Hosts receiving the advertisements will acquire other information through stateless autoconfiguration.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

The O flag in RA advertisements determines whether receiving hosts use stateful autoconfiguration to obtain configuration information other than IPv6 addresses.

- If the O flag is set to 1 in RA advertisements, receiving hosts use stateful autoconfiguration (for example, from a DHCPv6 server) to obtain configuration information other than IPv6 addresses.
- If the O flag is set to 0 in RA advertisements, receiving hosts use stateless autoconfiguration to obtain configuration information other than IPv6 addresses.

Examples

Set the O flag to 0 in RA advertisements to be sent.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] undo ipv6 nd autoconfig other-flag
```

ipv6 nd dad attempts

Use **ipv6 nd dad attempts** to set the number of attempts to send an NS message for DAD.

Use **undo ipv6 nd dad attempts** to restore the default.

Syntax

ipv6 nd dad attempts *times*

undo ipv6 nd dad attempts

Default

The number of attempts to send an NS message for DAD is 1.

Views

Interface view

Predefined user roles

network-admin

Parameters

times: Specifies the number of attempts to send an NS message for DAD, in the range of 0 to 600. If it is set to 0, DAD is disabled.

Usage guidelines

An interface sends an NS message for DAD after obtaining an IPv6 address.

If the interface does not receive a response within the time specified by using **ipv6 nd ns retrans-timer**, it resends an NS message.

If the interface receives no response after making the maximum sending attempts (set by using **ipv6 nd dad attempts**), the interface uses the obtained address.

Examples

Set the number of attempts to send an NS message for DAD to 20.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd dad attempts 20
```

Related commands

display ipv6 interface

ipv6 nd ns retrans-timer

ipv6 nd ns retrans-timer

Use **ipv6 nd ns retrans-timer** to set the interval for retransmitting an NS message.

Use **undo ipv6 nd ns retrans-timer** to restore the default.

Syntax

ipv6 nd ns retrans-timer *value*

undo ipv6 nd ns retrans-timer

Default

The local interface sends NS messages at every an interval of 1000 milliseconds, and the Retrans Timer field in the RA messages sent is 0. The interval for retransmitting an NS message is determined by the receiving device.

Views

Interface view

Predefined user roles

network-admin

Parameters

value: Specifies the interval value in the range of 1000 to 4294967295 milliseconds.

Usage guidelines

If a device does not receive a response from the peer within the specified interval, the device resends an NS message. The device retransmits an NS message at the specified interval and uses the interval value to fill the Retrans Timer field in RA messages to be sent.

Examples

Specify VLAN-interface 100 to retransmit NS messages every 10000 milliseconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ns retrans-timer 10000
```

Related commands

display ipv6 interface

ipv6 nd nud reachable-time

Use **ipv6 nd nud reachable-time** to set the neighbor reachable time on an interface.

Use **undo ipv6 nd nud reachable-time** to restore the default.

Syntax

ipv6 nd nud reachable-time *time*

undo ipv6 nd nud reachable-time

Default

The neighbor reachable time on the local interface is 1200000 milliseconds, and the value of the Reachable Time field in RA messages is 0. The reachable time is determined by the receiving device.

Views

Interface view

Predefined user roles

network-admin

Parameters

time: Specifies the neighbor reachable time in the range of 1 to 3600000 milliseconds.

Usage guidelines

If the neighbor reachability detection shows that a neighbor is reachable, the device considers the neighbor reachable within the specified reachable time. If the device must send a packet to the neighbor after the specified reachable time expires, the device reconfirms whether the neighbor is reachable. The device sets the specified value as the neighbor reachable time on the local interface and uses the value to fill the Reachable Time field in RA messages to be sent.

Examples

Set the neighbor reachable time on VLAN-interface 100 to 10000 milliseconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
```

```
[Sysname-Vlan-interface100] ipv6 nd nud reachable-time 10000
```

Related commands

display ipv6 interface

ipv6 nd online-offline-log enable

Use **ipv6 nd online-offline-log enable** to enable ND logging for user online and offline events.

Use **undo ipv6 nd online-offline-log enable** to disable ND logging for user online and offline events.

Syntax

ipv6 nd online-offline-log enable [**rate** *rate*]

undo ipv6 nd online-offline-log enable

Default

ND logging for user online and offline events is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

rate *rate*: Specifies the maximum number of logs that can be output per second. The value range is 10 to 300. If you do not specify this option, the maximum log output rate is 100 logs per second.

Usage guidelines

A higher log output rate consumes more CPU resources. Adjust the log output rate based the CPU performance and usage.

Examples

Enable ND logging for user online and offline events, and set the maximum log output rate to 100 logs per second.

```
<Sysname> system-view
[Sysname] ipv6 nd online-offline-log enable rate 100
```

Related commands

ipv6 neighbor

ipv6 nd ra boot-file-url

Use **ipv6 nd ra boot-file-url** to specify the URL of the boot file in RA messages.

Use **undo ipv6 nd ra boot-file-url** to restore the default.

Syntax

ipv6 nd ra boot-file-url *url-string*

undo ipv6 nd ra boot-file-url

Default

RA messages do not carry the URL of the boot file.

Views

Interface view

Predefined user roles

network-admin

Parameters

url-string: Specifies the URL address of the boot file, a case-sensitive string of 1 to 127 characters. The URL address must be started with http://, https://. ftp://, or tftp://.

Usage guidelines

In some specific networks, a device follows the steps to implement automatic configuration:

1. Obtains an IPv6 address through ND or DHCPv6.
2. Obtains the URL address for downloading the boot file from the DHCPv6 server.
3. Downloads the boot file from the FTP server and installs it.

With the boot file URL specified in RA messages, the device can use the ND protocol to obtain both the IPv6 address and the boot file URL for automatic configuration. DHCPv6 is not required in the network, simplifying the network deployment.

Examples

Specify the boot file URL address as tftp://169.254.0.1/file/softimg.iso in RA messages on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra boot-file-url tftp://169.254.0.1/file/softimg.iso
```

ipv6 nd ra dns search-list

Use **ipv6 nd ra dns search-list** to specify DNS suffix information to be advertised in RA messages.

Use **undo ipv6 nd ra dns search-list** to remove a DNS suffix from RA message advertisement.

Syntax

ipv6 nd ra dns search-list *domain-name* [*seconds* | **infinite**] **sequence** *seqno*

undo ipv6 nd ra dns search-list *domain-name*

Default

DNS suffix information is not specified and RA messages do not carry DNS suffix options.

Views

Interface view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a DNS suffix. It is a dot-separated, case-insensitive string that can include letters, digits, hyphens (-), underscores (_), and dots (.), for example, aabbcc.com. The

DNS suffix can include a maximum of 253 characters, and each separated string includes no more than 63 characters.

seconds: Specifies the lifetime of the DNS suffix, in seconds. The value range is 4 to 4294967295. Value 4294967295 indicates that the lifetime of the DNS suffix is infinite.

infinite: Sets the lifetime of the DNS suffix to infinite.

seqno: Specifies the sequence number of the DNS suffix, in the range of 0 to 4294967295. The sequence number for a DNS suffix must be unique. A smaller sequence number represents a higher priority.

Usage guidelines

The DNS search list (DNSSL) option in RA messages provides DNS suffix information for hosts. The RA messages allow hosts to obtain their IPv6 addresses and the DNS suffix through stateless autoconfiguration. This method is useful in a network where DHCPv6 infrastructure is not provided.

The default lifetime of the DNS suffix is three times the maximum interval for advertising RA messages. To set the maximum interval, use the **ipv6 nd ra interval** command.

You can configure a maximum of eight DNS suffixes on an interface. One DNSSL option contains one DNS suffix. All DNSSL options are sorted in ascending order of the sequence number of the DNS suffix.

The sequence number uniquely identifies a DNS suffix. To modify a DNS suffix or its sequence number, you must first use the **undo ipv6 nd ra dns search-list** command to remove the DNS suffix from RA message advertisement.

After you execute the **ipv6 nd ra dns search-list** command, the device immediately sends an RA message with the existing and newly specified DNS suffix information.

After you execute the **undo ipv6 nd ra dns search-list** command, the device immediately sends two RA messages.

- The first RA message carries information about all DNS suffixes, including DNS suffixes specified in the **undo** command with their lifetime set to 0 seconds.
- The second RA message carries information about remaining DNS suffixes.

Each time the device sends an RA message from an interface, it immediately refreshes the RA message advertisement interval for that interface.

Examples

Specify the DNS suffix as **com**, the suffix lifetime as **infinite**, and the sequence number as **1** for RA messages on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra dns search-list com infinite sequence 1
```

Related commands

ipv6 nd ra dns search-list suppress

ipv6 nd ra interval

ipv6 nd ra dns search-list suppress

Use **ipv6 nd ra dns search-list suppress** to enable DNS suffix suppression in RA messages.

Use **undo ipv6 nd ra dns search-list suppress** to disable DNS suffix suppression in RA messages.

Syntax

ipv6 nd ra dns search-list suppress

undo ipv6 nd ra dns search-list suppress

Default

DNS suffix suppression in RA messages is disabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

This command suppresses advertising DNS suffixes in RA messages.

RA messages are suppressed by default. To disable RA message suppression, use the **undo ipv6 nd ra halt** command.

Whether enabling this feature on an interface will trigger sending RA message immediately for DNS suffix update depends on the interface configuration:

- If the interface has been configured with DNS suffix information, the device immediately sends two RA messages. In the first message, the lifetime for DNS suffixes is 0 seconds. The second RA message does not carry any DNSSL options.
- If the interface has no DNS suffix information specified, no RA messages are triggered.
- If you specify a new DNS suffix or remove a DNS suffix, the device immediately sends an RA message without any DNSSL options.

Whether disabling this feature on an interface will trigger sending RA message immediately for DNS suffix update depends on the interface configuration:

- If the interface has been configured with the DNS suffix information, the device immediately sends an RA message carrying the DNS suffix information.
- If the interface has no DNS suffix information specified, no RA messages are triggered.

Each time the device sends an RA message from an interface, it immediately refreshes the RA message advertisement interval for that interface.

Examples

Enable DNS suffix suppression in RA messages on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra dns search-list suppress
```

Related commands

ipv6 nd ra dns search-list

ipv6 nd ra dns server

Use **ipv6 nd ra dns server** to specify DNS server information to be advertised in RA messages.

Use **undo ipv6 nd ra dns server** to remove a DNS server from RA message advertisement.

Syntax

ipv6 nd ra dns server *ipv6-address* [*seconds* | **infinite**] **sequence** *seqno*

undo ipv6 nd ra dns server *ipv6-address*

Default

DNS server information is not specified and RA messages do not carry DNS server options.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the IPv6 address of the DNS server, which must be a global unicast address or a link-local address.

seconds: Specifies the lifetime of the DNS server, in seconds. The value range is 4 to 4294967295. Value 4294967295 indicates that the lifetime of the DNS server is infinite.

infinite: Sets the lifetime of the DNS server to infinite.

sequence *seqno*: Specifies the sequence number of the DNS server, in the range of 0 to 4294967295. The sequence number for a DNS server must be unique. A smaller sequence number represents a higher priority.

Usage guidelines

The DNS server option in RA messages provides DNS server information for hosts. The RA messages allow hosts to obtain their IPv6 addresses and the DNS server through stateless autoconfiguration. This method is useful in a network where DHCPv6 infrastructure is not provided.

The default lifetime of the DNS server is three times the maximum interval for advertising RA messages. To set the maximum interval, use the **ipv6 nd ra interval** command.

You can configure a maximum of eight DNS servers on an interface. One DNS server option contains one DNS server. All DNS server options are sorted in ascending order of the DNS server sequence number.

The sequence number uniquely identifies a DNS server. To modify the IPv6 address or sequence number of a DNS server, you must first use the **undo ipv6 nd ra dns server** command to remove the DNS server from RA message advertisement.

After you execute the **ipv6 nd ra dns server** command, the device immediately sends an RA message with the existing and newly specified DNS server options.

After you execute the **undo ipv6 nd ra dns server** command, the device immediately sends two RA messages.

- The first RA message carries information about all DNS servers, including the DNS servers specified in the **undo** command with their lifetime set to 0 seconds.
- The second RA message carries information about remaining DNS servers.

Each time the device sends an RA message from an interface, it immediately refreshes the RA message advertisement interval for that interface.

Examples

Specify the DNS server address as **2001:10::100**, the server lifetime as **infinite**, and the sequence number as **1** for RA messages on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra dns server 2001:10::100 infinite sequence 1
```

Related commands

ipv6 nd ra dns server suppress

ipv6 nd ra interval

ipv6 nd ra dns server suppress

Use **ipv6 nd ra dns server suppress** to enable DNS server suppression in RA messages.

Use **undo ipv6 nd ra dns server suppress** to disable DNS server suppression in RA messages.

Syntax

ipv6 nd ra dns server suppress

undo ipv6 nd ra dns server suppress

Default

DNS server suppression in RA messages is disabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

This command suppresses advertising DNS server addresses in RA messages.

RA messages are suppressed by default. To disable RA message suppression, use the **undo ipv6 nd ra halt** command.

Whether enabling this feature on an interface will trigger sending RA message immediately for DNS server information update depends on the interface configuration:

- If the interface has been configured with DNS server information or has obtained an AAA-authorized DNS server address, the device immediately sends two RA messages. In the first message, the lifetime for DNS server addresses is 0 seconds. The second RA message does not carry any DNS server options.
- If the interface has no DNS server information specified or no AAA-authorized DNS server address assigned, no RA messages are triggered.
- If you specify a new DNS server or remove a DNS server, the device immediately sends an RA message without any DNS server address options.

Whether disabling this feature on an interface will trigger sending RA message immediately for DNS server information update depends on the interface configuration:

- If the interface has been configured with the DNS server information or has obtained an AAA-authorized DNS server address, the device immediately sends an RA message carrying the DNS server information.
- If the interface has no DNS server information specified or no AAA-authorized DNS server address assigned, no RA messages are triggered.

Each time the device sends an RA message from an interface, it immediately refreshes the RA message advertisement interval for that interface.

Examples

Enable DNS server suppression in RA messages on VLAN-interface 100.

```
<Sysname> system-view
```

```
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra dns server suppress
```

Related commands

ipv6 nd ra dns server

ipv6 nd ra halt

Use **ipv6 nd ra halt** to suppress an interface from advertising RA messages.

Use **undo ipv6 nd ra halt** to disable this feature.

Syntax

ipv6 nd ra halt

undo ipv6 nd ra halt

Default

An interface is suppressed from sending RA messages.

Views

Interface view

Predefined user roles

network-admin

Examples

Disable RA message suppression on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] undo ipv6 nd ra halt
```

ipv6 nd ra hop-limit unspecified

Use **ipv6 nd ra hop-limit unspecified** to specify unlimited hops in RA messages.

Use **undo ipv6 nd ra hop-limit unspecified** to restore the default.

Syntax

ipv6 nd ra hop-limit unspecified

undo ipv6 nd ra hop-limit unspecified

Default

The maximum number of hops in the RA messages is limited to 64.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

To set the maximum number of hops to a value rather than the default setting, use the **ipv6 hop-limit** command.

Examples

Specify unlimited hops in the RA messages on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ipv6 nd ra hop-limit unspecified
```

Related commands

ipv6 hop-limit

ipv6 nd ra interval

Use **ipv6 nd ra interval** to set the maximum and minimum intervals for advertising RA messages.

Use **undo ipv6 nd ra interval** to restore the default.

Syntax

ipv6 nd ra interval *max-interval min-interval*

undo ipv6 nd ra interval

Default

The maximum interval between RA messages is 600 seconds, and the minimum interval is 200 seconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

max-interval: Specifies the maximum interval value in seconds, in the range of 4 to 1800.

min-interval: Specifies the minimum interval value in the range of 3 seconds to three-fourths of the maximum interval.

Usage guidelines

The device advertises RA messages randomly between the maximum interval and the minimum interval.

The maximum interval for sending RA messages should be less than or equal to the router lifetime in RA messages.

Examples

Set the maximum interval for advertising RA messages to 1000 seconds and the minimum interval to 700 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra interval 1000 700
```

Related commands

ipv6 nd ra router-lifetime

ipv6 nd ra no-advlinkmtu

Use **ipv6 nd ra no-advlinkmtu** to turn off the MTU option in RA messages.

Use **undo ipv6 nd ra no-advlinkmtu** to restore the default.

Syntax

ipv6 nd ra no-advlinkmtu

undo ipv6 nd ra no-advlinkmtu

Default

RA messages contain the MTU option.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

The MTU option in the RA messages specifies the link MTU to ensure that all nodes on the link use the same MTU.

Examples

Turn off the MTU option in RA messages on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra no-advlinkmtu
```

ipv6 nd ra prefix

Use **ipv6 nd ra prefix** to configure the prefix information in RA messages.

Use **undo ipv6 nd ra prefix** to restore the default.

Syntax

ipv6 nd ra prefix { *ipv6-prefix prefix-length* | *ipv6-prefix*/*prefix-length* } [*valid-lifetime preferred-lifetime* [**no-autoconfig** | **off-link** | **prefix-preference** *level*] * | **no-advertise**]

undo ipv6 nd ra prefix { *ipv6-prefix* | *ipv6-prefix*/*prefix-length* }

Default

No prefix information is configured for RA messages. Instead, the IPv6 address of the interface sending RA messages is used as the prefix information.

If the IPv6 address is manually configured, the prefix uses the fixed valid lifetime 2592000 seconds (30 days) and preferred lifetime 604800 seconds (7 days).

If the IPv6 address is automatically obtained (through DHCP, for example), the prefix uses the valid and preferred lifetime of the IPv6 address.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-prefix: Specifies the IPv6 prefix.

prefix-length: Specifies the prefix length of the IPv6 address.

valid-lifetime: Specifies the valid lifetime of a prefix, in the range of 0 to 4294967295 seconds. The default value is 2592000 seconds (30 days).

preferred-lifetime: Specifies the preferred lifetime of a prefix used for stateless autoconfiguration, in the range of 0 to 4294967295 seconds. The preferred lifetime cannot be longer than the valid lifetime. The default value is 604800 seconds (7 days).

no-autoconfig: Specifies a prefix not to be used for stateless autoconfiguration. If you do not specify this keyword, the prefix is used for stateless autoconfiguration.

off-link: Indicates that the address with the prefix is not directly reachable on the link. If you do not specify this keyword, the address with the prefix is directly reachable on the link.

prefix-preference *level*: Specifies the prefix preference. The *level* argument specifies the preference value in the range of 0 to 255. A larger value indicates a higher preference. The client selects an IPv6 prefix with the highest preference for address generation. If you do not specify this option, the RA message does not carry the preference for the prefix.

no-advertise: Disables the device from advertising the prefix specified in this command. If you do not specify this keyword, the device advertises the prefix specified in this command.

Usage guidelines

After hosts on the same link receive RA messages, they can use the prefix information in the RA messages for stateless autoconfiguration.

A prefix specified without a parameter in this command preferentially uses the default settings configured by using the **ipv6 nd ra prefix default** command. If the default settings are unavailable, the prefix uses the following settings:

- Valid lifetime of 2592000 seconds (30 days).
- Preferred lifetime of 604800 seconds (7 days).
- The prefix is used for stateless autoconfiguration.
- The address with the prefix is directly reachable on the link.
- The prefix is advertised in RA messages.

Examples

Configure the prefix information in RA messages on VLAN-interface 100.

Method 1:

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra prefix 2001:10::100/64 100 10
```

Method 2:

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra prefix 2001:10::100 64 100 10
```

ipv6 nd ra prefix default

Use **ipv6 nd ra prefix default** to configure the default settings for prefixes advertised in RA messages.

Use **undo ipv6 nd ra prefix default** to restore the default.

Syntax

ipv6 nd ra prefix default [*valid-lifetime preferred-lifetime* [**no-autoconfig** | **off-link**] * | **no-advertise**]

undo ipv6 nd ra prefix default

Default

No default settings are configured for prefixes advertised in RA messages.

Views

Interface view

Predefined user roles

network-admin

Parameters

valid-lifetime: Specifies the valid lifetime of a prefix, in the range of 0 to 4294967295 seconds. The default value is 2592000 seconds (30 days).

preferred-lifetime: Specifies the preferred lifetime of a prefix used for stateless autoconfiguration, in the range of 0 to 4294967295 seconds. The preferred lifetime cannot be longer than the valid lifetime. The default value is 604800 seconds (7 days).

no-autoconfig: Specifies a prefix not to be used for stateless autoconfiguration. If you do not specify this keyword, the prefix is used for stateless autoconfiguration.

off-link: Indicates that the address with the prefix is not directly reachable on the link. If you do not specify this keyword, the address with the prefix is directly reachable on the link.

no-advertise: Disables the device from advertising the prefix specified in this command. If you do not specify this keyword, the device advertises the prefix specified in this command.

Usage guidelines

This command specifies the default settings for the prefix specified by using the **ipv6 nd ra prefix** command. If none of the parameters (*valid-lifetime*, *preferred-lifetime*, **no-autoconfig**, **off-link**, and **no-advertise**) is configured in the **ipv6 nd ra prefix** command, the prefix uses the default settings.

Examples

Configure the default settings for prefixes advertised in RA messages on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra prefix default 100 10
```

ipv6 nd ra router-lifetime

Use **ipv6 nd ra router-lifetime** to set the router lifetime in RA messages.

Use **undo ipv6 nd ra router-lifetime** to restore the default.

Syntax

ipv6 nd ra router-lifetime *time*

undo ipv6 nd ra router-lifetime

Default

The router lifetime in RA messages is three times the maximum interval for advertising RA messages.

Views

Interface view

Predefined user roles

network-admin

Parameters

time: Specifies the router lifetime in the range of 0 to 9000 seconds. If the value is set to 0, the router does not act as the default router.

Usage guidelines

The router lifetime in RA messages specifies how long the router sending the RA messages acts as the default router. Hosts receiving the RA messages check this value to determine whether to use the sending router as the default router. If the router lifetime is 0, the router cannot be used as the default router.

The router lifetime in RA messages must be greater than or equal to the advertising interval.

Examples

Set the router lifetime in RA messages on VLAN-interface 100 to 1000 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra router-lifetime 1000
```

Related commands

ipv6 nd ra interval

ipv6 nd router-preference

Use **ipv6 nd router-preference** to set a router preference in RA messages.

Use **undo ipv6 nd router-preference** to restore the default.

Syntax

ipv6 nd router-preference { **high** | **low** | **medium** }

undo ipv6 nd router-preference

Default

The router preference is **medium**.

Views

Interface view

Predefined user roles

network-admin

Parameters

high: Sets the router preference to the highest setting.

low: Sets the router preference to the lowest setting.

medium: Sets the router preference to the medium setting.

Usage guidelines

A hosts selects a router with the highest preference as the default router.

When router preferences are the same in RA messages, a host selects the router corresponding to the first received RA message as the default gateway.

Examples

Set the router preference in RA messages to the highest on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd router-preference high
```

ipv6 nd snooping dad retrans-timer

Use **ipv6 nd snooping dad retrans-timer** to set the interval for retransmitting an NS message for DAD.

Use **undo ipv6 nd snooping dad retrans-timer** to restore the default.

Syntax

ipv6 nd snooping dad retrans-timer *interval*

undo ipv6 nd snooping dad retrans-timer

Default

The interval for retransmitting an NS message for DAD is 250 milliseconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the interval for retransmitting an NS message for DAD, in the range of 100 to 500 milliseconds.

Usage guidelines

When creating, updating, or deleting an ND snooping entry, the device sends an NS message to test the entry by DAD. When both of the following conditions exist, the device retransmits an NS message by default:

- The device does not receive a reply within the retransmission interval.
- The retransmission interval is less than or equal to the timeout time for ND snooping entries in INVALID status (TENTATIVE, TESTING_TPLT, or TESTING_VP).

For the device to send the NS message only once, set a retransmission interval longer than the timeout time for ND snooping entries in INVALID status.

Example

Set the interval to 200 milliseconds for retransmitting an NS message for DAD.

```
<Sysname> system-view
[Sysname] ipv6 nd snooping dad retrans-timer 200
```

ipv6 nd snooping enable global

Use **ipv6 nd snooping enable global** to enable ND snooping for global unicast addresses.

Use **undo ipv6 nd snooping enable global** to disable ND snooping for global unicast addresses.

Syntax

ipv6 nd snooping enable global

undo ipv6 nd snooping enable global

Default

ND snooping is disabled for global unicast addresses.

Views

VLAN view

Predefined user roles

network-admin

Examples

Enable ND snooping for global unicast addresses.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] ipv6 nd snooping enable global
```

ipv6 nd snooping enable link-local

Use **ipv6 nd snooping enable link-local** to enable ND snooping for link-local addresses.

Use **undo ipv6 nd snooping enable link-local** to disable ND snooping for link-local addresses.

Syntax

ipv6 nd snooping enable link-local

undo ipv6 nd snooping enable link-local

Default

ND snooping is disabled for link-local addresses.

Views

VLAN view

Predefined user roles

network-admin

Examples

Enable ND snooping for link-local addresses.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] ipv6 nd snooping enable link-local
```

ipv6 nd snooping glean source

Use **ipv6 nd snooping glean source** to enable ND snooping for data packets from unknown sources.

Use **undo ipv6 nd snooping glean source** to disable ND snooping for data packets from unknown sources.

Syntax

ipv6 nd snooping glean source

undo ipv6 nd snooping glean source

Default

ND snooping is disabled for data packets from unknown sources.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

This command enables the device to learn ND snooping entries from data packets originated by unknown sources.

For this command to take effect, execute the **ipv6 nd snooping enable global** command or the **ipv6 nd snooping enable link-local** command.

Before enabling ND snooping entries learning from data packets for a VLAN, you must configure IPv6 source guard on all untrusted interfaces in the same VLAN. This operation ensures correct forwarding of the data packets received all these interfaces.

Examples

Enable ND snooping for data packets from unknown sources.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] ipv6 nd snooping glean source
```

ipv6 nd snooping lifetime

Use **ipv6 nd snooping lifetime** to set timeout timers for ND snooping entries.

Use **undo ipv6 nd snooping lifetime** to restore the default.

Syntax

ipv6 nd snooping lifetime { **invalid** *invalid-lifetime* | **valid** *valid-lifetime* }

undo ipv6 nd snooping lifetime { **invalid** | **valid** }

Default

The timeout timer for ND snooping entries in INVALID status (TENTATIVE, TESTING_TPLT, or TESTING_VP) is 500 milliseconds.

The timeout timer for ND snooping entries in VALID status is 300 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

invalid *invalid-lifetime*: Sets a timeout timer for ND snooping entries in INVALID status (TENTATIVE, TESTING_TPLT, or TESTING_VP). The value range is 250 to 1000 milliseconds.

valid *valid-lifetime*: Sets a timeout timer for ND snooping entries in VALID status. The value range is 60 to 900 seconds.

Examples

Set the timeout timer to 250 seconds for ND snooping entries in VALID status.

```
<Sysname> system-view
[Sysname] ipv6 nd snooping lifetime valid 250
```

ipv6 nd snooping max-learning-num

Use **ipv6 nd snooping max-learning-num** to set the ND snooping entry learning limit for an interface.

Use **undo ipv6 nd snooping max-learning-num** to restore the default.

Syntax

ipv6 nd snooping max-learning-num *max-number*

undo ipv6 nd snooping max-learning-num

Default

An interface can learn a maximum of 1024 ND snooping entries.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

max-number: Specifies the maximum number of ND snooping entries that an interface can learn. The value range for this argument is 1 to 1024.

Usage guidelines

An interface can learn ND snooping entries. The learning limit is limited by the ND snooping entry learning limit for all VLANs. To set the learning limit for all VLANs, use the **ipv6 nd snooping vlan max-learning-num** command.

Examples

Allow GigabitEthernet 1/0/1 to learn a maximum of 64 ND snooping entries.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd snooping max-learning-num 64
```

ipv6 nd snooping uplink

Use **ipv6 nd snooping uplink** to configure the port as an ND snooping uplink port. The ND snooping uplink port cannot learn ND snooping entries.

Use **undo ipv6 nd snooping uplink** to restore the default.

Syntax

ipv6 nd snooping uplink

undo ipv6 nd snooping uplink

Default

The port is not an ND snooping uplink port. After ND snooping is enabled, the port can learn ND snooping entries.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Examples

Configure GigabitEthernet 1/0/1 as an ND snooping uplink port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd snooping uplink
```

Configure Bridge-aggregation 1 as an ND snooping uplink port.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] ipv6 nd snooping uplink
```

ipv6 nd user-ip-conflict record enable

Use **ipv6 nd user-ip-conflict record enable** to enable recording user IPv6 address conflicts.

Use **undo ipv6 nd user-ip-conflict record enable** to disable recording user IPv6 address conflicts.

Syntax

ipv6 nd user-ip-conflict record enable

undo ipv6 nd user-ip-conflict record enable

Default

Recording user IPv6 address conflicts is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This feature detects and records user IPv6 address conflicts. A conflict occurs if an incoming NA packet has the same source IPv6 address as an existing ND entry but a different source MAC address. The device generates a user IPv6 address conflict record, logs the conflict, and sends the log to the information center. For information about the log destination and output rule configuration in the information center, see the information center in *Network Management and Monitoring Configuration Guide*.

Each IRF member device can generate a maximum of 10 user IPv6 address conflict logs per second. When this maximum number is reached, the member device suppresses generating user IPv6 address conflict logs and records the suppression times. Each IRF member device can save a maximum of 200 user IPv6 address conflict records.

When the number of saved user IPv6 address conflict records reaches the upper limit, new records overwrite old ones.

Examples

Enable recording user IPv6 address conflicts.

```
<Sysname> system-view
[Sysname] ipv6 nd user-ip-conflict record enable
```

Related commands

display ipv6 nd user-ip-conflict record

ipv6 nd user-move record enable

Use **ipv6 nd user-move record enable** to enable recording user port migrations.

Use **undo ipv6 nd user-move record enable** to disable recording user port migrations.

Syntax

ipv6 nd user-move record enable

undo ipv6 nd user-move record enable

Default

Recording user port migrations is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This feature enables the device to detect and record user port migrations. A user port migrates if an incoming NA packet has the same source IPv6 address and source MAC address as an existing ND entry but a different port. The device generates a user port migration record, logs the migration event, and sends the log to the information center. For information about the log destination and output rule configuration in the information center, see the information center in *Network Management and Monitoring Configuration Guide*.

Each IRF member device can generate a maximum of 10 user port migration logs per second. When this maximum number is reached, the member device suppresses generating user port migration logs and records the suppression times. Each IRF member device can save a maximum of 200 user port migration records.

When the number of saved user port migration records reaches the upper limit, new records overwrite old ones.

Examples

Enable recording user port migrations.

```
<Sysname> system-view
[Sysname] ipv6 nd user-move record enable
```

Related commands

display ipv6 nd user-move record

ipv6 neighbor

Use **ipv6 neighbor** to configure a static neighbor entry.

Use **undo ipv6 neighbor** to delete a neighbor entry.

Syntax

ipv6 neighbor *ipv6-address mac-address* { *vlan-id port-type port-number* | **interface** *interface-type interface-number* }

undo ipv6 neighbor *ipv6-address interface-type interface-number*

Default

No static neighbor entries exist.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the IPv6 address of the static neighbor entry.

mac-address: Specifies the MAC address (48 bits) of the static neighbor entry, in the format of H-H-H.

vlan-id: Specifies the VLAN ID of the static neighbor entry, in the range of 1 to 4094.

port-type port-number: Specifies a Layer 2 port of the static neighbor entry by its type and number.

interface *interface-type interface-number*: Specifies a Layer 3 interface of the static neighbor entry by its type and number.

Usage guidelines

A neighbor entry stores information about a link-local node. The entry can be created dynamically through NS and NA messages, or configured statically.

The device uniquely identifies a static neighbor entry by using the neighbor's IPv6 address and the number of the Layer 3 interface that connects to the neighbor. You can configure a static neighbor entry by using either of the following methods:

- **Method 1**—Associate a neighbor IPv6 address and link-layer address with the Layer 3 interface of the local node.
- **Method 2**—Associate a neighbor IPv6 address and link-layer address with a Layer 2 port in a VLAN containing the local node.

You can use either of the previous configuration methods to configure a static neighbor entry for a VLAN interface.

- If Method 1 is used, the neighbor entry is in INCMP state. After the device obtains the corresponding Layer 2 port information, the neighbor entry goes into REACH state.
- If Method 2 is used, the port specified by *port-type port-number* must belong to the VLAN specified by *vlan-id* and the corresponding VLAN interface must already exist. After the static neighbor entry is configured, the device associates the VLAN interface with the IPv6 address to uniquely identify the static neighbor entry. The entry will be in REACH state.

You can use the **undo ipv6 neighbor** command to delete both static and dynamic neighbor entries.

To delete a neighbor entry for a VLAN interface, specify only the corresponding VLAN interface.

Examples

Configure a static neighbor entry for VLAN-interface 1.

```
<Sysname> system-view
[Sysname] ipv6 neighbor 2000::1 fe-e0-89 interface Vlan-interface 1
```

Related commands

display ipv6 neighbors

reset ipv6 neighbors

ipv6 neighbor link-local minimize

Use **ipv6 neighbor link-local minimize** to minimize link-local ND entries.

Use **undo ipv6 neighbor link-local minimize** to restore the default.

Syntax

ipv6 neighbor link-local minimize

undo ipv6 neighbor link-local minimize

Default

All ND entries are assigned to the driver.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Perform this command to minimize link-local ND entries assigned to the driver. Link-local ND entries refer to ND entries that contain link-local addresses.

With this feature enabled, the device does not add newly learned link-local ND entries whose link local addresses are not the next hop of any route to the driver. This saves driver resources.

This feature affects only newly learned link-local ND entries rather than existing ND entries.

Examples

Minimize link-local ND entries.

```
<Sysname> system-view
[Sysname] ipv6 neighbor link-local minimize
```

ipv6 neighbor stale-aging

Use **ipv6 neighbor stale-aging** to set the aging timer for ND entries in stale state.

Use **undo ipv6 neighbor stale-aging** to restore the default.

Syntax

ipv6 neighbor stale-aging *aging-time*

undo ipv6 neighbor stale-aging

Default

The aging timer for ND entries in stale state is 240 minutes.

Views

System view

Predefined user roles

network-admin

Parameters

aging-time: Specifies the aging timer for ND entries in stale state, in the range of 1 to 1440 minutes.

Usage guidelines

This aging time applies to all ND entries in stale state. If an ND entry in stale state is not updated before the timer expires, it changes to the delay state. If it is still not updated in 5 seconds, the ND entry changes to the probe state. The device sends an NS message for detection a maximum of three attempts by default. If no response is received, the device deletes the ND entry.

You can set the aging timer for ND entries in stale state in system view and interface view. For ND entries in stale state on an interface, the aging timer in interface view has higher priority than the aging timer in system view.

Examples

Set the aging timer for ND entries in stale state to 120 minutes.

```
<Sysname> system-view
[Sysname] ipv6 neighbor stale-aging 120
```

Related commands

ipv6 neighbor timer stale-aging

ipv6 neighbor timer stale-aging

Use **ipv6 neighbor timer stale-aging** to set the aging timer for ND entries in stale state on an interface.

Use **undo ipv6 neighbor timer stale-aging** to restore the default.

Syntax

ipv6 neighbor timer stale-aging *aging-time*

undo ipv6 neighbor timer stale-aging

Default

The aging timer of ND entries in stale state is not configured on an interface. The aging timer is determined by the configuration of the **ipv6 neighbor stale-aging** command in system view.

Views

VLAN interface view

Predefined user roles

network-admin

Parameters

aging-time: Specifies the aging timer for ND entries in stale state on an interface. The value range is 1 to 1440 minutes.

Usage guidelines

This aging timer applies to ND entries in stale state on the interface. If an ND entry in stale state is not updated before the timer expires, it changes to the delay state. If it is still not updated in 5

seconds, the ND entry changes to the probe state. The device sends an NS message for probe and a maximum of three attempts is allowed by default. If no response is received, the device deletes the ND entry.

You can set the aging timer for ND entries in stale state in system view and interface view. For ND entries in stale state on an interface, the aging timer in interface view has higher priority than the aging timer in system view.

Examples

On VLAN-interface 2, set the aging timer to 200 minutes for ND entries in stale state.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ipv6 neighbor timer stale-aging 200
```

Related commands

ipv6 neighbor stale-aging

ipv6 neighbors max-learning-num

Use **ipv6 neighbors max-learning-num** to set the dynamic neighbor entry learning limit for an interface. This prevents the interface from occupying too many neighbor table resources.

Use **undo ipv6 neighbors max-learning-num** to restore the default.

Syntax

ipv6 neighbors max-learning-num *max-number*

undo ipv6 neighbors max-learning-num

Default

The following table describes the maximum number of dynamic neighbor entries that an interface can learn on different switches:

Hardware	Maximum value for an interface
S5000V3-EI switch series S5000V5-EI switch series S5000E-X switch series S5000X-EI switch series WAS6000 switch series	64
S5110V2 switch series S5110V2-SI switch series WS5810-WiNet switch series	128
S5120V2-LI switch series S5130S-LI switch series S5120V3-SI switch series MS4320V2 switch series MS4320 switch series	256
S3100V3-SI switch series	• 128: LS-3100V3-28TP-SI-H1, LS-3100V3-18TP-SI-H1, LS-3100V3-52TP-SI-H1, LS-3100V3-20TP-PWR-SI-H1 • 256: Other models.
MS4200 switch series	• 128: LS-MS4200-28TP-H1,

Hardware	Maximum value for an interface
	LS-MS4200-20TP-PWR-H1, LS-MS4200-18TP-H1 • 256: Other models.
WS5820-WiNet switch series	• 128: WS5820-28P-POE-WiNet • 256: Other models.
MS4300V2 switch series	• 128: MS4300V2-28P and MS4300V2-52P • 256: MS4300V2-10P
MS4320V3 switch series	• 128: MS4320V3-28P and MS4320V3-52P • 256: Other models.
S5120V3-LI switch series	• 128: o S5120V3-20P-LI o S5120V3-28P-LI o S5120V3-52P-LI o S5120V3-28P-PWR-LI o S5120V3-52P-PWR-LI • 256: Other models.

Views

Layer 2 interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

max-number: Specifies the maximum number of dynamic neighbor entries that an interface can learn. The following table describes the value ranges for this argument on different switch series:

Hardware	Maximum value for an interface
S5000V3-EI switch series S5000V5-EI switch series S5000E-X switch series S5000X-EI switch series WAS6000 switch series	0 to 64
S5110V2 switch series S5110V2-SI switch series WS5810-WiNet switch series	0 to 128
S5120V2-LI switch series S5130S-LI switch series S5120V3-SI switch series MS4320V2 switch series MS4320 switch series	0 to 256
S3100V3-SI switch series	• 0 to 128: LS-3100V3-28TP-SI-H1, LS-3100V3-18TP-SI-H1, LS-3100V3-52TP-SI-H1,

Hardware	Maximum value for an interface
	LS-3100V3-20TP-PWR-SI-H1 • 0 to 256: Other models.
MS4200 switch series	• 0 to 128: LS-MS4200-28TP-H1, LS-MS4200-20TP-PWR-H1, LS-MS4200-18TP-H1 • 0 to 256: Other models.
WS5820-WiNet switch series	• 0 to 128: WS5820-28P-POE-WiNet • 0 to 256: Other models.
MS4300V2 switch series	• 0 to 128: MS4300V2-28P and MS4300V2-52P • 0 to 256: MS4300V2-10P
MS4320V3 switch series	• 0 to 128: MS4320V3-28P and MS4320V3-52P • 0 to 256: Other models.

S5120V3-LI switch series	• 0 to 128:
	  ○ S5120V3-20P-LI
	  ○ S5120V3-28P-LI
	  ○ S5120V3-52P-LI
	  ○ S5120V3-28P-PWR-LI
	  ○ S5120V3-52P-LI
	• 0 to 256: Other models.

Usage guidelines

The device can dynamically acquire the link-layer address of a neighboring node through NS and NA messages and add it into the neighbor table.

When the number of dynamic neighbor entries reaches the learning limit on an interface, the interface stops learning neighbor information.

Examples

Allow VLAN-interface 100 to learn a maximum of 10 dynamic neighbor entries.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 neighbors max-learning-num 10
```

ipv6 pathmtu

Use **ipv6 pathmtu** to set a static Path MTU for an IPv6 address.

Use **undo ipv6 pathmtu** to delete the Path MTU configuration for an IPv6 address.

Syntax

ipv6 pathmtu *ipv6-address value*

undo ipv6 pathmtu *ipv6-address*

Default

No static Path MTU is set.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies an IPv6 address.

value: Specifies the Path MTU of the specified IPv6 address, in the range of 1280 to 10240 bytes.

Usage guidelines

You can set a static Path MTU for a destination IPv6 address. When a source host sends a packet through an interface, it compares the interface MTU with the static Path MTU of the specified destination IPv6 address. If the packet size is larger than the smaller one of the two values, the host fragments the packet according to the smaller value.

Examples

Set a static Path MTU for an IPv6 address.

```
<Sysname> system-view
[Sysname] ipv6 pathmtu fe80::12 1300
```

Related commands

display ipv6 pathmtu

reset ipv6 pathmtu

ipv6 pathmtu age

Use **ipv6 pathmtu age** to set the aging time for a dynamic Path MTU.

Use **undo ipv6 pathmtu age** to restore the default.

Syntax

ipv6 pathmtu age *age-time*

undo ipv6 pathmtu age

Default

The aging time for dynamic Path MTU is 10 minutes.

Views

System view

Predefined user roles

network-admin

Parameters

age-time: Specifies the aging time for Path MTU in minutes, in the range of 10 to 100.

Usage guidelines

After the path MTU from a source host to a destination host is dynamically determined, the source host sends subsequent packets to the destination host based on this MTU. After the aging time expires, the following events occur:

- The dynamic Path MTU is removed.
- The source host determines a dynamic path MTU through the Path MTU mechanism again.

The aging time is invalid for a static Path MTU.

Examples

Set the aging time for a dynamic Path MTU to 40 minutes.

```
<Sysname> system-view
[Sysname] ipv6 pathmtu age 40
```

Related commands

display ipv6 pathmtu

ipv6 prefer temporary-address

Use **ipv6 prefer temporary-address** to enable the system to preferentially use the temporary IPv6 address of the sending interface as the source address of a packet.

Use **undo ipv6 prefer temporary-address** to disable the system to preferentially use the temporary IPv6 address of the sending interface as the source address of a packet.

Syntax

ipv6 prefer temporary-address

undo ipv6 prefer temporary-address

Default

The system is disabled to preferentially use the temporary IPv6 address of the sending interface as the source address of a packet.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The temporary address feature enables the system to generate and preferentially use the temporary IPv6 address of the sending interface as the source address of a packet. If the temporary IPv6 address cannot be used because of a DAD conflict, the system uses the public IPv6 address.

Examples

Enable the system to preferentially use the temporary IPv6 address of the sending interface as the source address of the packet.

```
<Sysname> system-view
[Sysname] ipv6 prefer temporary-address
```

Related commands

ipv6 address auto

ipv6 nd ra prefix

ipv6 temporary-address

ipv6 prefix

Use **ipv6 prefix** to configure a static IPv6 prefix.

Use **undo ipv6 prefix** to delete a static IPv6 prefix.

Syntax

ipv6 prefix *prefix-number ipv6-prefix/prefix-length*

undo ipv6 prefix *prefix-number*

Default

No static IPv6 prefix is configured.

Views

System view

Predefined user roles

network-admin

Parameters

prefix-number: Specifies a prefix ID in the range of 1 to 1024.

ipv6-prefix/prefix-length: Specifies a prefix and its length. The value range for the *prefix-length* argument is 1 to 128.

Usage guidelines

To modify an existing static prefix, execute the **undo ipv6 prefix** command to delete the existing static prefix, and then execute the **ipv6 prefix** command.

Dynamic IPv6 prefixes obtained from DHCPv6 servers cannot be manually removed or modified.

A static IPv6 prefix can have the same prefix ID with a dynamic IPv6 prefix, but the static one takes precedence over the dynamic one.

Examples

Create static IPv6 prefix 2001:0410::/32 with prefix ID 1.

```
<Sysname> system-view
[Sysname] ipv6 prefix 1 2001:0410::/32
```

Related commands

display ipv6 prefix

ipv6 reassemble local enable

Use **ipv6 reassemble local enable** to enable IPv6 local fragment reassembly.

Use **undo ipv6 reassemble local enable** to disable IPv6 local fragment reassembly.

Syntax

ipv6 reassemble local enable

undo ipv6 reassemble local enable

Default

IPv6 local fragment reassembly is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Configure this command on a multichassis IRF fabric to improve fragment reassembly efficiency. The command enables the subordinate to reassemble the IPv6 fragments of a packet if all the

fragments arrive at it. If this feature is disabled, all IPv6 fragments are delivered to the master for reassembly. The command applies only to fragments destined for the same subordinate.

Examples

Enable IPv6 local fragment reassembly.

```
<Sysname> system-view
[Sysname] ipv6 reassemble local enable
```

ipv6 redirects enable

Use **ipv6 redirects enable** to enable sending ICMPv6 redirect messages.

Use **undo ipv6 redirects enable** to disable sending ICMPv6 redirect messages.

Syntax

ipv6 redirects enable

undo ipv6 redirects enable

Default

Sending ICMPv6 redirect messages is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The default gateway sends an ICMPv6 redirect message to the source of an IPv6 packet to inform the source of a better first hop.

Sending ICMPv6 redirect messages enables hosts that hold few routes to establish routing tables and find the best route. Because this feature adds host routes into the routing tables, host performance degrades when there are too many host routes. As a result, sending ICMPv6 redirect messages is disabled by default.

Examples

Enable sending ICMPv6 redirect messages.

```
<Sysname> system-view
[Sysname] ipv6 redirects enable
```

ipv6 temporary-address

Use **ipv6 temporary-address** to enable the temporary IPv6 address feature.

Use **undo ipv6 temporary-address** to restore the default.

Syntax

ipv6 temporary-address [*valid-lifetime preferred-lifetime*]

undo ipv6 temporary-address

Default

The system does not generate any temporary IPv6 address.

Views

System view

Predefined user roles

network-admin

Parameters

valid-lifetime: Specifies the valid lifetime for temporary IPv6 addresses, in the range of 600 to 4294967295 seconds. The default valid lifetime is 604800 seconds (7 days).

preferred-lifetime: Specifies the preferred lifetime for temporary IPv6 addresses, in the range of 600 to 4294967295 seconds. The default preferred lifetime is 86400 seconds (1 day).

Usage guidelines

You must enable stateless autoconfiguration before enabling the temporary address feature.

The valid lifetime for temporary IPv6 addresses must be greater than or equal to the preferred lifetime for temporary IPv6 addresses.

In stateless address autoconfiguration, an interface automatically generates an IPv6 global unicast address by using the address prefix in the received RA message and the interface ID. On an IEEE 802 interface (such as an Ethernet interface or a VLAN interface), the interface ID is generated based on the interface's MAC address and is globally unique. An attacker can exploit this rule to easily identify the sending device.

To fix the vulnerability, you can enable the temporary address feature. An IEEE 802 interface generates the following addresses:

- **Public IPv6 address**—Includes an address prefix in the RA message and a fixed interface ID generated based on the interface's MAC address.
- **Temporary IPv6 address**—Includes an address prefix in the RA message and a random interface ID generated through MD5.

When the valid lifetime of a temporary IPv6 address expires, the system deletes the address and generates a new one. This enables the system to send packets with different source addresses through the same interface. The preferred lifetime and valid lifetime for a temporary IPv6 address are determined as follows:

- The preferred lifetime of a temporary IPv6 address takes the smaller of the following values:
  - The preferred lifetime of the address prefix in the RA message.
  - The preferred lifetime configured for temporary IPv6 addresses minus DESYNC_FACTOR (a random number in the range of 0 to 600 seconds).
- The valid lifetime of a temporary IPv6 address takes the smaller of the following values:
  - The valid lifetime of the address prefix.
  - The valid lifetime configured for temporary IPv6 addresses.

Examples

Enable the system to generate a temporary IPv6 address.

```
<Sysname> system-view
[Sysname] ipv6 temporary-address
```

Related commands

ipv6 address auto

ipv6 nd ra prefix

ipv6 prefer temporary-address

ipv6 unreachables enable

Use **ipv6 unreachables enable** to enable sending ICMPv6 destination unreachable messages.

Use **undo ipv6 unreachables** to disable sending ICMPv6 destination unreachable messages.

Syntax

ipv6 unreachables enable

undo ipv6 unreachables enable

Default

Sending ICMPv6 destination unreachable messages is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

If the device fails to forward a received IPv6 packet because of a destination unreachable error, it performs the following operations:

- Drops the packet.
- Sends an ICMPv6 destination unreachable message to the source.

If the device is generating ICMPv6 destination unreachable messages incorrectly, disable sending ICMPv6 destination unreachable messages to prevent attack risks.

Examples

Enable sending ICMPv6 destination unreachable messages.

```
<Sysname> system-view
[Sysname] ipv6 unreachables enable
```

local-proxy-nd enable

Use **local-proxy-nd enable** to enable local ND proxy.

Use **undo local-proxy-nd enable** to disable local ND proxy.

Syntax

local-proxy-nd enable

undo local-proxy-nd enable

Default

Local ND proxy is disabled.

Views

VLAN interface view

Predefined user roles

network-admin

Examples

Enable local ND proxy on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] local-proxy-nd enable
```

Related commands

proxy-nd enable

proxy-nd enable

Use **proxy-nd enable** to enable common ND proxy.

Use **undo proxy-nd enable** to disable common ND proxy.

Syntax

proxy-nd enable

undo proxy-nd enable

Default

Common ND proxy is disabled.

Views

VLAN interface view

Predefined user roles

network-admin

Examples

Enable common ND proxy on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] proxy-nd enable
```

Related commands

local-proxy-nd enable

reset ipv6 nd snooping vlan

Use **reset ipv6 nd snooping vlan** to clear ND snooping entries in VLANs.

Syntax

reset ipv6 nd snooping vlan { [*vlan-id*] [**global** | **link-local**] | *vlan-id ipv6-address* }

Views

User view

Predefined user roles

network-admin

Parameters

vlan-id: Clears ND snooping entries for the specified VLAN. The value range for the VLAN ID is 1 to 4094.

global: Clears ND snooping entries for global unicast addresses.

link-local: Clears ND snooping entries for link-local addresses.

vlan-id ipv6-address: Clears the ND snooping entry of the specified IPv6 address in the specified VLAN.

Usage guidelines

If you do not specify any parameters, this command clears ND snooping entries in all VLANs.

Examples

Clear ND snooping entries in all VLANs.

```
<Sysname> reset ipv6 nd snooping vlan
```

Related commands

display ipv6 nd snooping count vlan
display ipv6 nd snooping vlan

reset ipv6 neighbors

Use **reset ipv6 neighbors** to clear IPv6 neighbor information.

Syntax

reset ipv6 neighbors { **all** | **dynamic** | **interface** *interface-type interface-number* | **slot** *slot-number* | **static** }

Views

User view

Predefined user roles

network-admin

Parameters

all: Clears static and dynamic neighbor information for all interfaces.

dynamic: Clears dynamic neighbor information for all interfaces.

interface *interface-type interface-number*: Clears dynamic neighbor information for the interface specified by its type and number.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears dynamic neighbor information for all member devices.

static: Clears static neighbor information for all interfaces.

Examples

Clear neighbor information for all interfaces.

```
<Sysname> reset ipv6 neighbors all
This will delete all the entries. Continue? [Y/N]:Y
```

Clear dynamic neighbor information for all interfaces.

```
<Sysname> reset ipv6 neighbors dynamic
This will delete all the dynamic entries. Continue? [Y/N]:Y
```

Clear all neighbor information for GigabitEthernet 1/0/1.

```
<Sysname> reset ipv6 neighbors interface gigabitethernet 1/0/1
This will delete all the dynamic entries by the interface you specified. Continue? [Y/N]:Y
```

Related commands

display ipv6 neighbors

ipv6 neighbor

reset ipv6 pathmtu

Use **reset ipv6 pathmtu** to clear the Path MTU information.

Syntax

reset ipv6 pathmtu { **all** | **dynamic** | **static** }

Views

User view

Predefined user roles

network-admin

Parameters

all: Clears all Path MTUs.

dynamic: Clears all dynamic Path MTUs.

static: Clears all static Path MTUs.

Examples

Clear all Path MTUs.

```
<Sysname> reset ipv6 pathmtu all
```

Related commands

display ipv6 pathmtu

reset ipv6 statistics

Use **reset ipv6 statistics** to clear IPv6 and ICMPv6 packet statistics.

Syntax

reset ipv6 statistics [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears IPv6 and ICMPv6 packet statistics for all member devices.

Examples

Clear IPv6 and ICMPv6 packet statistics.

```
<Sysname> reset ipv6 statistics
```

Related commands

display ipv6 statistics

Contents

DHCPv6 commands

Common DHCPv6 commands

display ipv6 dhcp duid

Use **display ipv6 dhcp duid** to display the DUID of the local device.

Syntax

display ipv6 dhcp duid

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

A DHCP unique identifier (DUID) uniquely identifies a DHCPv6 device (DHCPv6 client, server, or relay agent). A DHCPv6 device adds its DUID in a sent packet.

This command displays output only after the DHCPv6 process is running on the device.

Examples

Display the DUID of the local device.

```
<Sysname> display ipv6 dhcp duid
The DUID of this device: 0003000100e0fc005552.
```

ipv6 dhcp advertise pd-route

Use **ipv6 dhcp advertise pd-route** to enable the DHCPv6 server or DHCPv6 relay agent to advertise IPv6 prefixes.

Use **undo ipv6 dhcp advertise pd-route** to disable the DHCPv6 server or DHCPv6 relay agent from advertising IPv6 prefixes.

Syntax

ipv6 dhcp advertise pd-route

undo ipv6 dhcp advertise pd-route

Default

The DHCPv6 server or DHCPv6 relay agent does not advertise IPv6 prefixes.

Views

System view

Predefined user roles

network-admin

Usage guidelines

A DHCPv6 client can obtain an IPv6 prefix through DHCPv6 and use the IPv6 prefix for IPv6 address assignment in a downstream network. If the IPv6 prefix is in a different subnet than the IPv6 address of the DHCPv6 client's upstream interface, the downstream network cannot access the external network. You can use this command to configure the DHCPv6 server or DHCPv6 relay agent, whichever is on the same link as the DHCPv6 client, to advertise the IPv6 prefix.

To use this command on the DHCPv6 relay agent, you must enable the DHCPv6 relay agent to record DHCPv6 relay entries first.

Examples

Enable the DHCPv6 server to advertise IPv6 prefixes.

```
<Sysname> system-view
[Sysname] ipv6 dhcp advertise pd-route
```

ipv6 dhcp dscp

Use **ipv6 dhcp dscp** to set the DSCP value for the DHCPv6 packets sent by the DHCPv6 server or the DHCPv6 relay agent.

Use **undo ipv6 dhcp dscp** to restore the default.

Syntax

ipv6 dhcp dscp *dscp-value*

undo ipv6 dhcp dscp

Default

The DSCP value is 56 in DHCPv6 packets sent by the DHCPv6 server or the DHCPv6 relay agent.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies the DSCP value for DHCPv6 packets, in the range of 0 to 63.

Usage guidelines

The DSCP value of a packet specifies the priority level of the packet and affects the transmission priority of the packet. A bigger DSCP value represents a higher priority.

Examples

Set the DSCP value to 30 for DHCPv6 packets sent by the DHCPv6 server or the DHCPv6 relay agent.

```
<Sysname> system-view
[Sysname] ipv6 dhcp dscp 30
```

ipv6 dhcp log enable

Use **ipv6 dhcp log enable** to enable DHCPv6 server logging.

Use **undo ipv6 dhcp log enable** to disable DHCPv6 server logging.

Syntax

ipv6 dhcp log enable

undo ipv6 dhcp log enable

Default

DHCPv6 server logging is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command enables the DHCPv6 server to generate DHCPv6 logs and send them to the information center. The log information helps administrators locate and solve problems. For information about the log destination and output rule configuration in the information center, see *Network Management and Monitoring Configuration Guide*.

As a best practice, disable this feature if the log generation affects the device performance or reduces the address and prefix allocation efficiency. For example, this situation might occur when a large number of clients frequently come online or go offline.

Examples

Enable DHCPv6 server logging.

```
<Sysname> system-view
[Sysname] ipv6 dhcp log enable
```

ipv6 dhcp select

Use **ipv6 dhcp select** to enable the DHCPv6 server or DHCPv6 relay agent on an interface.

Use **undo ipv6 dhcp select** to restore the default.

Syntax

ipv6 dhcp select { **relay** | **server** }

undo ipv6 dhcp select

Default

An interface does not work in the DHCPv6 server mode or in the DHCPv6 relay agent mode. It discards DHCPv6 packets from DHCPv6 clients.

Views

Interface view

Predefined user roles

network-admin

Parameters

relay: Enables the DHCPv6 relay agent on the interface.

server: Enables the DHCPv6 server on the interface.

Usage guidelines

Before changing the DHCPv6 server mode to the DHCPv6 relay agent mode on an interface, use the following commands to remove IPv6 address/prefix bindings:

- **reset ipv6 dhcp server ip-in-use**
- **reset ipv6 dhcp server pd-in-use**

Do not configure the DHCPv6 client on the interface that has been configured as the DHCPv6 relay agent or DHCPv6 server.

Examples

Enable the DHCPv6 server on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ipv6 dhcp select server
```

Enable the DHCPv6 relay agent on VLAN-interface 20.

```
<Sysname> system-view
[Sysname] interface vlan-interface 20
[Sysname-Vlan-interface20] ipv6 dhcp select relay
```

Related commands

display ipv6 dhcp relay server-address

display ipv6 dhcp server

DHCPv6 server commands

NOTE:

S5110V2-SI, S5000V3-EI, S5000V5-EI, S5000E-X, S5000X-EI, and WAS6000 do not support the DHCPv6 server functionality.

address range

Use **address range** to specify a non-temporary IPv6 address range in a DHCPv6 address pool for dynamic allocation.

Use **undo address range** to restore the default.

Syntax

address range *start-ipv6-address end-ipv6-address* [**preferred-lifetime** *preferred-lifetime* **valid-lifetime** *valid-lifetime*]

undo address range

Default

No non-temporary IPv6 address range exists.

Views

DHCPv6 address pool view

Predefined user roles

network-admin

Parameters

start-ipv6-address: Specifies the start IPv6 address.

end-ipv6-address: Specifies the end IPv6 address.

preferred-lifetime *preferred-lifetime*: Specifies the preferred lifetime for the non-temporary IPv6 addresses. The value range is 60 to 4294967295 seconds, and the default is 604800 seconds (7 days).

valid-lifetime *valid-lifetime*: Specifies the valid lifetime for the non-temporary IPv6 addresses. The value range is 60 to 4294967295 seconds, and the default is 2592000 seconds (30 days). The valid lifetime cannot be shorter than the preferred lifetime.

Usage guidelines

If you do not specify a non-temporary IPv6 address range, all unicast addresses on the subnet specified by the **network** command in address pool view are assignable. If you specify a non-temporary IPv6 address range, only the IPv6 addresses in the specified IPv6 address range are assignable.

You can specify only one non-temporary IPv6 address range in an address pool. If you execute this command multiple times, the most recent configuration takes effect.

The non-temporary IPv6 address range specified by the **address range** command must be on the subnet specified by the **network** command.

Examples

Configure a non-temporary IPv6 address range from 3ffe:501:ffff:100::10 through 3ffe:501:ffff:100::31 in address pool 1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] network 3ffe:501:ffff:100::/64
[Sysname-dhcp6-pool-1] address range 3ffe:501:ffff:100::10 3ffe:501:ffff:100::31
```

Related commands

display ipv6 dhcp pool

network

temporary address range

address-alloc-mode eui-64

Use **address-alloc-mode eui-64** to enable the EUI-64 address allocation mode.

Use **undo address-alloc-mode eui-64** to restore the default.

Syntax

address-alloc-mode eui-64

undo address-alloc-mode eui-64

Default

The EUI-64 address allocation mode is disabled. The DHCPv6 server does not allocates IPv6 addresses based on EUI-64.

Views

DHCPv6 address pool view

Predefined user roles

network-admin

Usage guidelines

The IPv6 leases that are allocated before the command execution are not affected.

This command takes effect when the prefix length of the IPv6 subnet does not exceed 64 in the DHCPv6 address pools.

This feature enables the DHCPv6 server to obtain the client MAC address from the link layer header of the DHCP request and generates an EUI-64 IPv6 address for the client. If a DHCPv6 relay agent is between the clients and server, do not configure this feature because the server cannot obtain the MAC addresses from received DHCP requests.

Examples

Enable the EUI-64 address allocation mode in DHCPv6 address pool **pool1**.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool pool1
[Sysname-dhcp6-pool-pool1] address-alloc-mode eui-64
```

class pool

Use **class pool** to specify a DHCPv6 address pool for a DHCPv6 user class.

Use **undo class pool** to restore the default.

Syntax

class *class-name* **pool** *pool-name*

undo class *class-name* **pool**

Default

No DHCPv6 address pool is specified for a DHCPv6 user class.

Views

DHCPv6 policy view

Predefined user roles

network-admin

Parameters

class-name: Specifies a DHCPv6 user class by its name, a case-insensitive string of 1 to 63 characters.

pool-name: Specifies a DHCPv6 address pool by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can specify only one DHCPv6 address pool for a DHCPv6 user class in a DHCPv6 policy. If you execute this command multiple times for a user class, the most recent configuration takes effect.

Examples

Specify DHCPv6 address pool **pool1** for DHCPv6 user class **test** in DHCPv6 policy 1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp policy 1
[Sysname-dhcp6-policy-1] class test pool pool1
```

Related commands

default pool

ipv6 dhcp policy

ipv6 dhcp pool

default pool

Use **default pool** to specify the default DHCPv6 address pool.

Use **undo default pool** to restore the default.

Syntax

default pool *pool-name*

undo default pool

Default

No default DHCPv6 address pool is specified.

Views

DHCPv6 policy view

Predefined user roles

network-admin

Parameters

pool-name: Specifies a DHCPv6 address pool by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

In a DHCPv6 policy, the DHCPv6 server uses the default address pool to assign IPv6 address, IPv6 prefix, or other parameters to clients that do not match any user classes. If no default address pool is specified or the default address pool does not have assignable IPv6 addresses or prefixes, the assignment fails.

You can specify only one default address pool in a DHCPv6 policy. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the DHCPv6 address pool **pool1** as the default DHCPv6 address pool in DHCPv6 policy 1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp policy 1
[Sysname-dhcp6-policy-1] default pool pool1
```

Related commands

class pool

ipv6 dhcp policy

display ipv6 dhcp option-group

Use **display ipv6 dhcp option-group** to display information about a DHCPv6 option group.

Syntax

display ipv6 dhcp option-group [*option-group-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

option-group-number: Specifies a static or dynamic DHCPv6 option group by its ID. The value range for the option group ID is 1 to 100. If you do not specify an option group, this command displays information about all DHCPv6 option groups.

Usage guidelines

A static DHCPv6 option group is created by using the **ipv6 dhcp option-group** command.

A dynamic DHCPv6 option group is created automatically by a DHCPv6 client after it obtains the DHCPv6 configuration parameters. Dynamic option groups cannot be manually modified or deleted.

Examples

Display information about all DHCPv6 option groups.

```
<Sysname> display ipv6 dhcp option-group
DHCPv6 option group: 1
  DNS server addresses:
    Type: Static
    Interface: N/A
    1::1
  DNS server addresses:
    Type: Dynamic (DHCPv6 address allocation)
    Interface: Vlan-interface10
    1::1
  Domain name:
    Type: Static
    Interface: N/A
    aaa.com
  Domain name:
    Type: Dynamic (DHCPv6 address allocation)
    Interface: Vlan-interface10
    aaa.com
  Options:
    Code: 23
      Type: Dynamic (DHCPv6 prefix allocation)
      Interface: Vlan-interface10
      Length: 2 bytes
      Hex: ABCD
DHCPv6 option group: 20
  DNS server addresses:
    Type: Static
    Interface: N/A
    1::1
  DNS server addresses:
    Type: Dynamic (DHCPv6 address allocation)
    Interface: Vlan-interface10
    1::1
  Domain name:
    Type: Static
    Interface: N/A
```

```
    aaa.com
  Domain name:
    Type: Dynamic (DHCPv6 address allocation)
    Interface: Vlan-interface10
    aaa.com
  Options:
    Code: 23
      Type: Dynamic (DHCPv6 prefix allocation)
      Interface: Vlan-interface10
      Length: 2 bytes
      Hex: ABCD
```

Table 1 Command output

Field	Description
DHCPv6 option group	ID of the DHCPv6 option group.
Type	Types of the DHCPv6 option: • **Static**—Parameter in a static DHCPv6 option group. • **Dynamic (DHCPv6 address allocation)**—Parameter in a dynamic DHCPv6 option group created during IPv6 address acquisition. • **Dynamic (DHCPv6 prefix allocation)**—Parameters in a dynamic DHCPv6 option group created during IPv6 prefix acquisition. • **Dynamic (DHCPv6 address and prefix allocation)**—Parameters in a dynamic DHCPv6 option group created during IPv6 address and prefix acquisition.
Interface	Interface name.
DNS server addresses	IPv6 address of the DNS server.
Domain name	Domain name suffix.
SIP server addresses	IPv6 address of the SIP server.
SIP server domain names	Domain name of the SIP server.
Options	Self-defined options.
Code	Code of the self-defined option.
Length	Self-defined option length in bytes.
Hex	Self-defined option content represented by a hexadecimal number.

Related commands

ipv6 dhcp option-group

display ipv6 dhcp pool

Use **display ipv6 dhcp pool** to display information about a DHCPv6 address pool.

Syntax

display ipv6 dhcp pool [*pool-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

pool-name: Displays information about the specified DHCPv6 address pool. The pool name is a case-insensitive string of 1 to 63 characters. If you do not specify a DHCPv6 address pool, this command displays information about all DHCPv6 address pools.

Examples

Display information about DHCPv6 address pool 1.

```
<Sysname> display ipv6 dhcp pool 1
DHCPv6 pool: 1
  Network: 3FFE:501:FFFF:100::/64
    Preferred lifetime 604800 seconds, valid lifetime 2592000 seconds
  Prefix pool: 1
    Preferred lifetime 24000 seconds, valid lifetime 36000 seconds
  Addresses:
    Range: from 3FFE:501:FFFF:100::1
           to 3FFE:501:FFFF:100::99
    Preferred lifetime 70480 seconds, valid lifetime 200000 seconds
    Total address number: 153
    Available: 153
    In-use: 0
  Temporary addresses:
    Range: from 3FFE:501:FFFF:100::200
           to 3FFE:501:FFFF:100::210
    Preferred lifetime 60480 seconds, valid lifetime 259200 seconds
    Total address number: 17
    Available: 17
    In-use: 0
  Static bindings:
    DUID: 0003000100e0fc000001
    IAID: 0000003f
    Prefix: 3FFE:501:FFFF:200::/64
      Preferred lifetime 604800 seconds, valid lifetime 2592000 seconds
    DUID: 0003000100e0fc00cff1
    IAID: 00000001
    Address: 3FFE:501:FFFF:2001::1/64
      Preferred lifetime 604800 seconds, valid lifetime 2592000 seconds
  DNS server addresses:
    2::2
  Domain name:
    aaa.com
  SIP server addresses:
    5::1
  SIP server domain names:
    bbb.com
```

Display information about DHCPv6 address pool 1.

```
<Sysname> display ipv6 dhcp pool 1
DHCPv6 pool: 1
  Network: Not-available
    Preferred lifetime 604800 seconds, valid lifetime 2592000 seconds
```

Display information about DHCPv6 address pool 1.

```
<Sysname> display ipv6 dhcp pool 1
DHCPv6 pool: 1
  Network: 1::/64(Zombie)
    Preferred lifetime 604800 seconds, valid lifetime 2592000 seconds
```

Table 2 Command output

Field	Description
DHCPv6 pool	Name of the DHCPv6 address pool.
Network	IPv6 subnet for dynamic IPv6 address allocation. If the subnet prefix is ineffective, this field displays **Not-available**. If the subnet prefix becomes ineffective after a configuration recovery, the prefix is marked **(Zombie)**.
Prefix pool	Prefix pool referenced by the address pool.
Preferred lifetime	Preferred lifetime in seconds.
valid lifetime	Valid lifetime in seconds.
Addresses	Non-temporary IPv6 address range.
Range	IPv6 address range for dynamic allocation.
Total address number	Total number of IPv6 addresses.
Available	Total number of available IPv6 addresses.
In-use	Total number of assigned IPv6 addresses.
Temporary addresses	Temporary IPv6 address range for dynamic allocation.
Static bindings	Static bindings configured in the address pool.
DUID	Client DUID.
IAID	Client IAID. If no IAID is configured, this field displays **Not configured**.
Prefix	IPv6 address prefix.
Address	Static IPv6 address.
DNS server addresses	DNS server address.
Domain name	Domain name.
SIP server addresses	SIP server address.
SIP server domain names	Domain name of the SIP server.

display ipv6 dhcp prefix-pool

Use **display ipv6 dhcp prefix-pool** to display information about a prefix pool.

Syntax

display ipv6 dhcp prefix-pool [*prefix-pool-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

prefix-pool-number: Displays detailed information about a prefix pool specified by its number in the range of 1 to 128. If you do not specify a prefix pool, this command displays brief information about all prefix pools.

Examples

Display brief information about all prefix pools.

```
<Sysname> display ipv6 dhcp prefix-pool
Prefix-pool Prefix                                  Available In-use Static
1           5::/64                                  64        0      0
```

Display brief information about all prefix pools.

```
<Sysname> display ipv6 dhcp  prefix-pool
Prefix-pool Prefix                                  Available In-use Static
2           Not-available                           0         0      0
```

Display brief information about all prefix pools.

```
<Sysname> display ipv6 dhcp  prefix-pool
Prefix-pool Prefix                                  Available In-use Static
11          21::/112(Zombie)                        0         64     0
```

Display detailed information about prefix pool 1.

```
<Sysname> display ipv6 dhcp prefix-pool 1
Prefix: 5::/64
Assigned length: 70
Total prefix number: 64
Available: 64
In-use: 0
Static: 0
```

Display detailed information about prefix pool 1.

```
<Sysname> display ipv6 dhcp prefix-pool 1
Prefix: Not-available
Assigned length: 70
Total prefix number: 0
Available: 0
In-use: 0
Static: 0
```

Display detailed information about prefix pool 1.

```
<Sysname> display ipv6 dhcp prefix-pool 1
Prefix: 5::/64(Zombie)
Assigned length: 70
Total prefix number: 10
Available: 0
In-use: 10
```

```
Static: 0
```

Table 3 Command output

Field	Description
Prefix-pool	Prefix pool number.
Prefix	Prefix specified in the prefix pool. If the prefix is ineffective, this field displays **Not-available**. If the prefix becomes ineffective after a configuration recovery, the prefix is marked **(Zombie)**.
Available	Number of available prefixes.
In-use	Number of assigned prefixes.
Static	Number of statically bound prefixes.
Assigned length	Length of assigned prefixes.
Total prefix number	Number of prefixes.

display ipv6 dhcp server

Use **display ipv6 dhcp server** to display DHCPv6 server configuration information.

Syntax

display ipv6 dhcp server [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Displays DHCPv6 server configuration information for the specified interface. If you do not specify an interface, this command displays DHCPv6 server configuration information for all interfaces.

Examples

Display DHCPv6 server configuration information for all interfaces.

```
<Sysname> display ipv6 dhcp server
Interface                     Pool
Vlan-interface2               1
Vlan-interface3               global
```

Display DHCPv6 server configuration information for the interface VLAN-interface 2.

```
<Sysname> display ipv6 dhcp server interface vlan-interface 2
Using pool: 1
Preference value: 0
Allow-hint: Enabled
Rapid-commit: Disabled
```

Table 4 Command output

Field	Description
Interface	Interface enabled with DHCPv6 server.
Pool	Address pool applied to the interface. If no address pool is applied to the interface, **global** is displayed. The DHCPv6 server selects a global address pool to assign a prefix, an address, and other configuration parameters to a client.
Using pool	Address pool applied to the interface. If no address pool is applied to the interface, **global** is displayed. The DHCPv6 server selects a global address pool to assign a prefix, an address, and other configuration parameters to a client.
Preference value	Server preference in the DHCPv6 Advertise message. The value range is 0 to 255. The bigger the value is, the higher preference the server has.
Allow-hint	Indicates whether desired address/prefix assignment is enabled.
Rapid-commit	Indicates whether rapid address/prefix assignment is enabled.

display ipv6 dhcp server conflict

Use **display ipv6 dhcp server conflict** to display information about IPv6 address conflicts.

Syntax

display ipv6 dhcp server conflict [**address** *ipv6-address*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

address *ipv6-address*: Displays conflict information for the specified IPv6 address. If you do not specify an IPv6 address, this command displays information about all IPv6 address conflicts.

Usage guidelines

The DHCPv6 server creates IP address conflict information in the following conditions:

- The DHCPv6 client sends a DECLINE packet to the DHCPv6 server to inform the server of an IPv6 address conflict.
- The DHCPv6 server discovers that the only assignable address in the address pool is its own IPv6 address.

Examples

Display information about all address conflicts.

```
<Sysname> display ipv6 dhcp server conflict
IPv6 address                                Detect time
2001::1                                     Apr 25 16:57:20 2007
1::1:2                                      Apr 25 17:00:10 2007
```

Table 5 Command output

Field	Description
IPv6 address	Conflicted IPv6 address.
Detect time	Time when the conflict was discovered.

Related commands

`reset ipv6 dhcp server conflict`

display ipv6 dhcp server database

Use **`display ipv6 dhcp server database`** to display information about DHCPv6 binding auto backup.

Syntax

`display ipv6 dhcp server database`

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display information about DHCPv6 binding auto backup.

```
<Sysname> display ipv6 dhcp server database
 File name               :   database.dhcp
 Username                :
 Password                :
 Update interval         :   600 seconds
 Latest write time       :   Feb  8 16:02:23 2014
 Status                  :   Last write succeeded.
```

Table 6 Command output

Field	Description
File name	Name of the DHCPv6 binding backup file.
Username	Username for accessing the URL of the remote backup file.
Password	Password for accessing the URL of the remote backup file. This field displays ********** if a password is configured.
Update interval	Waiting time in seconds after a DHCPv6 binding change for the DHCPv6 server to update the backup file.
Latest write time	Time of the latest update.
Status	Status of the update: • **Writing**—The backup file is being updated. • **Last write succeeded**—The backup file was successfully updated. • **Last write failed**—The backup file failed to be updated.

display ipv6 dhcp server expired

Use **display ipv6 dhcp server expired** to display lease expiration information.

Syntax

display ipv6 dhcp server expired [**address** *ipv6-address* | **pool** *pool-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

address *ipv6-address*: Displays lease expiration information for the specified IPv6 address. If you do not specify an IPv6 address, this command displays lease expiration information for all IPv6 addresses.

pool *pool-name*: Displays lease expiration information for the DHCPv6 address pool specified by its name, a case-insensitive string of 1 to 63 characters. If you do not specify a DHCPv6 address pool, this command displays lease expiration information for all DHCPv6 address pools.

Usage guidelines

DHCPv6 assigns the expired IPv6 addresses to DHCPv6 clients when all available addresses have been assigned.

Examples

Display all lease expiration information.

```
<Sysname> display ipv6 dhcp server expired
IPv6 address           DUID                          Lease expiration
2001:3eff:fe80:4caa:   3030-3066-2e65-3230-302e-     Apr 25 17:10:47 2007
37ee:7::1              3130-3234-2d45-7468-6572-
                       6e65-7430-2f31
```

Table 7 Command output

Field	Description
IPv6 address	Expired IPv6 address.
DUID	Client DUID bound to the expired IPv6 address.
Lease expiration	Time when the lease expired.

Related commands

reset ipv6 dhcp server expired

display ipv6 dhcp server ip-in-use

Use **display ipv6 dhcp server ip-in-use** to display binding information for assigned IPv6 addresses.

Syntax

display ipv6 dhcp server ip-in-use [**address** *ipv6-address* | **pool** *pool-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

address *ipv6-address*: Displays binding information for the specified IPv6 address. If you do not specify an IPv6 address, this command displays binding information for all IPv6 addresses.

pool *pool-name*: Displays IPv6 address binding information for the DHCPv6 address pool specified by its name, a case-insensitive string of 1 to 63 characters. If you do not specify a DHCPv6 address pool, this command displays IPv6 address binding information for all DHCPv6 address pools.

Examples

Display binding information for all assigned IPv6 address.

```
<Sysname> display ipv6 dhcp server ip-in-use
Pool: 1
 IPv6 address                            Type     Lease expiration
 2:1::1                                  Auto(O)  Jul 10 19:45:01 2008
Pool: 2
 IPv6 address                            Type      Lease expiration
 1:1::2                                  Static(F) Not available
Pool: 3
 IPv6 address                            Type      Lease expiration
 1:2::1F1                                Static(O) Oct  9 09:23:31 2008
Pool: 4
 IPv6 address                            Type      Lease expiration
 1:2::2                                  Auto(Z)   Oct  11 09:23:31 2008
```

Display binding information for all assigned IPv6 addresses for the specified DHCPv6 address pool.

```
<Sysname> display ipv6 dhcp server ip-in-use pool 1
Pool: 1
 IPv6 address                            Type      Lease expiration
 2:1::1                                  Auto(O)   Jul 10 22:22:22 2008
 3:1::2                                  Static(C) Jan  1 11:11:11 2008
```

Display binding information for the specified IPv6 address.

```
<Sysname> display ipv6 dhcp server ip-in-use address 2:1::3
Pool: 1
Client: FE80::C800:CFF0:FE18:0
Type: Auto(O)
DUID: 00030001CA000C180000
IAID: 0x00030001
  IPv6 address: 2:1::3
  Preferred lifetime 400, valid lifetime 500
  Expires at Jul 10 09:45:01 2008 (288 seconds left)
```

Table 8 Command output

Field	Description
Pool	DHCPv6 address pool.
IPv6 address	IPv6 address assigned.
Type	IPv6 address binding types: • **Static(F)**—Free static binding whose IPv6 address has not been assigned. • **Static(O)**—Offered static binding whose IPv6 address has been selected and sent by the DHCPv6 server in a DHCPv6-OFFER packet to the client. • **Static(C)**—Committed static binding whose IPv6 address has been assigned to the client. • **Auto(O)**—Offered dynamic binding whose IPv6 address has been dynamically selected by the DHCPv6 server and sent in a DHCPv6-OFFER packet to the DHCPv6 client. • **Auto(C)**—Committed dynamic binding whose IPv6 address has been dynamically assigned to the DHCPv6 client. • **Auto(Z)**—Zombie dynamic binding whose IPv6 address has been dynamically assigned to the DHCPv6 client. The binding becomes zombie because the subnet prefix goes invalid for address allocation after a configuration recovery.
Lease-expiration	Time when the lease of the IPv6 address will expire. If the lease expires after the year 2100, this field displays **Expires after 2100**. For an unassigned static binding, this field displays **Not available**.
Client	IPv6 address of the DHCPv6 client. For an unassigned static binding, this field is blank.
DUID	Client DUID.
IAID	Client IAID. For an unassigned static binding without IAID specified, this field displays **N/A**.
Preferred lifetime	Preferred lifetime in seconds of the IPv6 address.
valid lifetime	Valid lifetime in seconds of the IPv6 address.
Expires at	Time when the lease of an IPv6 address will expire. If the lease expires after the year 2100, this field displays **Expires after 2100**.

Related commands

`reset ipv6 dhcp server ip-in-use`

display ipv6 dhcp server pd-in-use

Use **`display ipv6 dhcp server pd-in-use`** to display binding information for the assigned IPv6 prefixes.

Syntax

`display ipv6 dhcp server pd-in-use` [**`pool`** *`pool-name`* | **`prefix`** *`prefix/prefix-len`*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

pool *pool-name*: Displays IPv6 prefix binding information for the DHCPv6 address pool specified by its name, a case-insensitive string of 1 to 63 characters. If you do not specify a DHCPv6 address pool, this command displays IPv6 prefix binding information for all DHCPv6 address pools.

prefix *prefix/prefix-len*: Displays binding information for the specified IPv6 prefix. The value range for the prefix length is 1 to 128. If you do not specify an IPv6 prefix, this command displays binding information for all IPv6 prefixes.

Examples

Display all IPv6 prefix binding information.

```
<Sysname> display ipv6 dhcp server pd-in-use
Pool: 1
 IPv6 prefix                              Type      Lease expiration
 2:1::/24                                 Auto(O)   Jul 10 19:45:01 2008
Pool: 2
 IPv6 prefix                              Type      Lease expiration
 1:1::/64                                 Static(F) Not available
Pool: 3
 IPv6 prefix                              Type      Lease expiration
 1:2::/64                                 Static(O) Oct  9 09:23:31 2008
Pool: 4
 IPv6 prefix                              Type      Lease expiration
 12::/80                                  Auto(Z)   Oct 17 09:34:59 2008
```

Display IPv6 prefix binding information for DHCPv6 address pool 1.

```
<Sysname> display ipv6 dhcp server pd-in-use pool 1
Pool: 1
 IPv6 prefix                              Type      Lease expiration
 2:1::/24                                 Auto(O)   Jul 10 22:22:22 2008
 3:1::/64                                 Static(C) Jan  1 11:11:11 2008
```

Display binding information for the IPv6 prefix 2:1::3/24.

```
<Sysname> display ipv6 dhcp server pd-in-use prefix 2:1::3/24
Pool: 1
Client: FE80::C800:CFF:FE18:0
Type: Auto(O)
DUID: 00030001CA000C180000
IAID: 0x00030001
  IPv6 prefix: 2:1::/24
  Preferred lifetime 400, valid lifetime 500
  Expires at Jul 10 09:45:01 2008 (288 seconds left)
```

Table 9 Command output

Field	Description
IPv6 prefix	IPv6 prefix assigned.

Field	Description
Type	Prefix binding types: • **Static(F)**—Free static binding whose IPv6 prefix has not been assigned. • **Static(O)**—Offered static binding whose IPv6 prefix has been selected and sent by the DHCPv6 server in a DHCPv6-OFFER packet to the client. • **Static(C)**—Committed static binding whose IPv6 prefix has been assigned to the client. • **Auto(O)**—Offered dynamic binding whose IPv6 prefix has been dynamically selected by the DHCPv6 server and sent in a DHCPv6-OFFER packet to the DHCPv6 client. • **Auto(C)**—Committed dynamic binding whose IPv6 prefix has been dynamically assigned to the DHCPv6 client. • **Auto(Z)**—Zombie dynamic binding whose IPv6 prefix has been dynamically assigned to the DHCPv6 client. The binding becomes zombie because the prefix in the prefix pool goes invalid after a configuration recovery.
Pool	Address pool.
Lease-expiration	Time when the lease of the IPv6 prefix will expire. If the lease will expire after the year 2100, this field displays **Expires after 2100**. For an unassigned static binding, this field displays **Not available**.
Client	IPv6 address of the DHCPv6 client. For an unassigned static binding, this field is blank.
DUID	Client DUID.
IAID	Client IAID. For an unassigned static binding without IAID, this field displays **N/A**.
Preferred lifetime	Preferred lifetime in seconds of the IPv6 prefix.
valid lifetime	Valid lifetime in seconds of the IPv6 prefix.
Expires at	Time when the lease of the prefix will expire. If the lease expires after the year 2100, this field displays **Expires after 2100**.

Related commands

reset ipv6 dhcp server pd-in-use

display ipv6 dhcp server statistics

Use **display ipv6 dhcp server statistics to** display DHCPv6 packet statistics on the DHCPv6 server.

Syntax

display ipv6 dhcp server statistics [**pool** *pool-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

pool *pool-name*: Displays DHCPv6 packet statistics for the DHCPv6 address pool specified by its name, a case-insensitive string of 1 to 63 characters. If you do not specify an address pool, this command displays DHCPv6 packet statistics for all address pools.

Examples

Display all DHCPv6 packet statistics on the DHCPv6 server.

```
<Sysname> display ipv6 dhcp server statistics
Bindings:
    Ip-in-use               :  1
    Pd-in-use               :  0
    Expired                 :  0
Conflict                    :  0
Packets received            :  1
    Solicit                 :  1
    Request                 :  0
    Confirm                 :  0
    Renew                   :  0
    Rebind                  :  0
    Release                 :  0
    Decline                 :  0
    Information-request     :  0
    Relay-forward           :  0
Packets dropped             :  0
Packets sent                :  0
    Advertise               :  0
    Reconfigure             :  0
    Reply                   :  0
    Relay-reply             :  0
```

Table 10 Command output

Field	Description
Bindings	Number of bindings: • **Ip-in-use**—Total number of address bindings. • **Pd-in-use**—Total number of prefix bindings. • **Expired**—Total number of expired address bindings.
Conflict	Total number of conflicted addresses. If statistics about an address pool are displayed, this field is not displayed.

Field	Description
Packets received	Number of messages received by the DHCPv6 server. The message types include: • Solicit. • Request. • Confirm. • Renew. • Rebind. • Release. • Decline. • Information-request. • Relay-forward. If statistics about an address pool are displayed, this field is not displayed.
Packets dropped	Number of packets discarded. If statistics about an address pool are displayed, this field is not displayed.
Packets sent	Number of messages sent by the DHCPv6 server. The message types include: • Advertise. • Reconfigure. • Reply. • Relay-reply. If statistics about an address pool are displayed, this field is not displayed.

Related commands

`reset ipv6 dhcp server statistics`

dns-server

Use **`dns-server`** to specify a DNS server in a DHCPv6 address pool.

Use **`undo dns-server`** to remove the specified DNS server from a DHCPv6 address pool.

Syntax

`dns-server` *`ipv6-address`*

`undo dns-server` *`ipv6-address`*

Default

No DNS server address is specified.

Views

DHCPv6 address pool view

DHCPv6 option group view

Predefined user roles

network-admin

Parameters

`ipv6-address`: Specifies the IPv6 address of a DNS server.

Usage guidelines

You can use the **`dns-server`** command to specify up to eight DNS servers in an address pool. A DNS server specified earlier has a higher preference.

Examples

Specify the DNS server address 2:2::3 in DHCPv6 address pool 1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] dns-server 2:2::3
```

Related commands

display ipv6 dhcp pool

domain-name

Use **domain-name** to specify a domain name in a DHCPv6 address pool.

Use **undo domain-name** to restore the default.

Syntax

domain-name *domain-name*

undo domain-name

Default

No domain name is specified.

Views

DHCPv6 address pool view

DHCPv6 option group view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a domain name, a case-sensitive string of 1 to 50 characters.

Usage guidelines

You can configure only one domain name in an address pool. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the domain name **aaa.com** in DHCPv6 address pool 1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] domain-name aaa.com
```

Related commands

display ipv6 dhcp pool

if-match

Use **if-match** to configure a match rule for a DHCPv6 user class.

Use **undo if-match** to delete a match rule for a DHCP user class.

Syntax

if-match rule *rule-number* { **option** *option-code* [**ascii** *ascii-string* [**offset** *offset* | **partial**] | **hex** *hex-string* [**mask** *mask* | **offset** *offset* **length** *length* | **partial**]] | **relay-agent** *gateway-ipv6-address* }

undo if-match rule *rule-number*

Default

No match rules are configured for the DHCPv6 user class.

Views

DHCPv6 user class view

Predefined user roles

network-admin

Parameters

rule *rule-number*: Assigns the match rule an ID in the range of 1 to 16. A smaller ID represents a higher match priority.

option *option-code*: Specifies a DHCPv6 option by its number in the range of 1 to 65535.

ascii *ascii-string*: Specifies an ASCII string of 1 to 128 characters.

offset *offset*: Specifies the offset in bytes after which the match operation starts. The value range is 0 to 65534. If you specify an ASCII string, a packet matches the rule if the option content after the offset is the same as the ASCII string. If you specify a hexadecimal number, a packet matches the rule if the option content of the specified length after the offset is the same as the hexadecimal number.

partial: Enables partial match. A packet matches the rule if the specified option in the packet contains the ASCII string or hexadecimal number specified in the rule. For example, if you specify **abc** in the rule, option content **xabc**, **xyzabca**, **xabcyz**, and **abcxyz** all match the rule.

hex *hex-string*: Specifies a hexadecimal number. The length of the hexadecimal number must be an even number in the range of 2 to 256.

mask *mask*: Specifies the mask for the match operation. The mask is a hexadecimal number whose length is an even number in the range of 2 to 256 and must be the same as the *hex-string* length. The DHCPv6 server selects option content of the mask length from the start and ANDs the selected option content and the specified hexadecimal number with the mask. The packet matches the rule if the two AND operation results are the same.

length *length*: Specifies the length of the option content to be matched, in the range of 1 to 128 bytes. The length must be the same as the *hex-string* length.

relay-agent *gateway-ipv6-address*: Specifies a **link-address** field value. The value is an IPv6 address. A packet matches the rule if its **link-address** field value is the same as that in the rule.

Usage guidelines

If a DHCPv6 request sent by a DHCPv6 client matches a rule in a DHCPv6 user class, the DHCPv6 client matches the user class.

You can configure multiple match rules for a DHCPv6 user class. Each match rule is uniquely identified by a rule ID within its type (option or relay agent address).

- If the rule that you are configuring has the same ID and type as an existing rule, the new rule overwrites the existing rule.
- If the rule that you are configuring has the same ID as an existing rule but a different type, the new rule takes effect and coexists with the existing rule. As a best practice, do not assign the same ID to rules of different types.

- Rules of different IDs cannot have the same rule content.

When you configure an **if-match option** rule, follow these guidelines:

- To match packets that contain an option, specify only the *option-code* argument.
- To match a hexadecimal number by AND operations, specify the **option** *option-code* **hex** *hex-string* **mask** *mask* options.
- To match a hexadecimal number directly, specify the **option** *option-code* **hex** *hex-string* [**offset** *offset* **length** *length* | **partial**] options. If you do not specify the **offset**, **length**, or **partial** parameter, a packet matches a rule if the option content starts with the hexadecimal number.
- To match an ASCII string, specify the **option** *option-code* **ascii** *ascii-string* [**offset** *offset* | **partial**] options. If you do not specify the **offset** or **partial** parameter, a packet matches a rule if the option content starts with the ASCII string.

Examples

Configure match rule **1** for the DHCPv6 user class **exam** to match DHCPv6 requests that contain Option 16.

```
<Sysname> system-view
[Sysname] ipv6 dhcp class exam
[Sysname-dhcp6-class-exam] if-match rule 1 option 16
```

Configure match rule **2** for the DHCPv6 user class **exam**. The rule matches DHCPv6 requests in which the highest bit of the fourth byte in Option 16 is the hexadecimal number **1**.

```
<Sysname> system-view
[Sysname] ipv6 dhcp class exam
[Sysname-dhcp6-class-exam] if-match rule 2 option 16 hex 00000080 mask 00000080
```

Configure match rule **3** for the DHCPv6 user class **exam**. The rule matches DHCPv6 requests in which the first three bytes of Option 16 are the hexadecimal number **13ae92**.

```
<Sysname> system-view
[Sysname] ipv6 dhcp class exam
[Sysname-dhcp6-class-exam] if-match rule 3 option 16 hex 13ae92 offset 0 length 3
```

Configure match rule **4** for the DHCPv6 user class **exam**. The rule matches DHCPv6 requests in which the Option 16 contains the hexadecimal number **13ae**.

```
<Sysname> system-view
[Sysname] ipv6 dhcp class exam
[Sysname-dhcp6-class-exam] if-match rule 5 option 16 hex 13ae partial
```

Configure match rule **5** for the DHCPv6 user class **exam** to match DHCPv6 requests in which the **link-address** field is 2001::1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp class exam
[Sysname-dhcp6-class-exam] if-match rule 5 relay-agent 2001::1
```

Related commands

ipv6 dhcp class

ipv6 dhcp apply-policy

Use **ipv6 dhcp apply-policy** to apply a DHCPv6 policy to an interface.

Use **undo ipv6 dhcp apply-policy** to restore the default.

Syntax

ipv6 dhcp apply-policy *policy-name*

undo ipv6 dhcp apply-policy

Default

No DHCPv6 policy is applied to an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a DHCPv6 policy by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can apply only one DHCPv6 policy to an interface. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Apply the DHCPv6 policy **test** to VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ipv6 dhcp apply-policy test
```

Related commands

ipv6 dhcp class

ipv6 dhcp class

Use **ipv6 dhcp class** to create a DHCPv6 user class and enter its view, or enter the view of an existing DHCPv6 user class.

Use **undo ipv6 dhcp class** to delete the specified DHCPv6 user class.

Syntax

ipv6 dhcp class *class-name*

undo ipv6 dhcp class *class-name*

Default

No DHCPv6 user classes exist.

Views

System view

Predefined user roles

network-admin

Parameters

class-name: Specifies a name for the DHCPv6 user class, a case-insensitive string of 1 to 63 characters.

Usage guidelines

In the DHCPv6 user class view, you can use the **if-match** command to configure match rules for user classification.

Examples

Create a DHCPv6 user class **test** and enter DHCPv6 user class view.

```
<Sysname> system-view
[Sysname] ipv6 dhcp class test
[Sysname-dhcp6-class-test]
```

Related commands

class pool

ipv6 dhcp policy

if-match

ipv6 dhcp option-group

Use **ipv6 dhcp option-group** to create a static DHCPv6 option group and enter its view.

Use **undo ipv6 dhcp option-group** to delete the specified static DHCPv6 option group.

Syntax

ipv6 dhcp option-group *option-group-number*

undo ipv6 dhcp option-group *option-group-number*

Default

No static DHCPv6 option groups exist.

Views

System view

Predefined user roles

network-admin

Parameters

option-group-number: Assigns an ID to the static option group, in the range of 1 to 100.

Usage guidelines

A static DHCPv6 option group can use the same ID as a dynamic DHCPv6 option group. If a static DHCPv6 option group and a dynamic DHCPv6 option group use the same ID, the static one takes precedence over the dynamic one.

Examples

Create static DHCPv6 option group 1 and enter its view.

```
<Sysname> system-view
[Sysname] ipv6 dhcp option-group 1
[Sysname-dhcp6-option-group-1]
```

Related commands

display ipv6 dhcp option-group

ipv6 dhcp policy

Use **ipv6 dhcp policy** to create a DHCPv6 policy and enter its view, or enter the view of an existing DHCPv6 policy.

Use **undo ipv6 dhcp policy** to delete a DHCPv6 policy.

Syntax

ipv6 dhcp policy *policy-name*

undo ipv6 dhcp policy *policy-name*

Default

No DHCPv6 policies exist.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Assigns a name to the DHCPv6 policy. The policy name is a case-insensitive string of 1 to 63 characters.

Usage guidelines

In DHCP policy view, you can specify address pools for different user classes. Clients matching a user class will obtain IPv6 addresses and other parameters from the specified address pool.

For a DHCPv6 policy to take effect, you must apply it to an interface.

Examples

Create DHCPv6 policy **test** and enter its view.

```
<Sysname> system-view
[Sysname] ipv6 dhcp policy test
[Sysname-dhcp6-policy-test]
```

Related commands

class pool

default pool

ipv6 dhcp apply-policy

ipv6 dhcp class

ipv6 dhcp pool

Use **ipv6 dhcp pool** to create a DHCPv6 address pool and enter its view, or enter the view of an existing DHCPv6 address pool.

Use **undo ipv6 dhcp pool** to delete the specified DHCPv6 address pool.

Syntax

ipv6 dhcp pool *pool-name*

undo ipv6 dhcp pool *pool-name*

Default

No DHCPv6 address pools exist.

Views

System view

Predefined user roles

network-admin

Parameters

pool-name: Specifies a name for the DHCPv6 address pool, a case-insensitive string of 1 to 63 characters.

Usage guidelines

A DHCPv6 address pool stores IPv6 address/prefix and other configuration parameters to be assigned to DHCPv6 clients.

When you delete a DHCPv6 address pool, binding information for the assigned IPv6 addresses and prefixes in the address pool is also deleted.

Examples

Create a DHCPv6 address pool named **pool1** and enter its view.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool pool1
[Sysname-dhcp6-pool-pool1]
```

Related commands

class pool

display ipv6 dhcp pool

ipv6 dhcp server apply pool

ipv6 dhcp prefix-pool

Use **ipv6 dhcp prefix-pool** to create a prefix pool and specify the prefix and the assigned prefix length for the pool.

Use **undo ipv6 dhcp prefix-pool** to delete the specified prefix pool.

Syntax

ipv6 dhcp prefix-pool *prefix-pool-number* **prefix** { *prefix-number* | *prefix/prefix-len* } **assign-len** *assign-len*

undo ipv6 dhcp prefix-pool *prefix-pool-number*

Default

No prefix pools exist.

Views

System view

Predefined user roles

network-admin

Parameters

prefix-pool-number: Specifies a prefix pool number in the range of 1 to 128.

prefix { *prefix-number* | *prefix/prefix-len* }: Specifies a prefix by its ID or in the format of *prefix*/*prefix length*. The value range for the *prefix-number* argument is 1 to 1024. The value range for the *prefix-len* argument is 1 to 128.

assign-len *assign-len*: Specifies the assigned prefix length. The value range is 1 to 128, and the value must be greater than or equal to *prefix-len*. The difference between *assign-len* and *prefix-len* must be no more than 16.

Usage guidelines

Different prefix pools cannot overlap.

To modify a prefix pool, execute the **undo ipv6 dhcp prefix-pool** command to delete the prefix pool, and then execute the **ipv6 dhcp prefix-pool** command.

Deleting a prefix pool clears all prefix bindings from the prefix pool.

When you specify a prefix by its ID, follow these restrictions and guidelines:

- This command does not take effect if the prefix does not exist. This command takes effect after the prefix is created.
- If the prefix that the ID represents is changed, the prefix range in the prefix pool accordingly changes.

Examples

Create IPv6 prefix 88:99::/32 with ID 3. Configure prefix pool 2 with IPv6 prefix 3 and an assigned prefix length of 42. Prefix pool 2 contains 1024 prefixes from 88:99::/42 to 88:99:FFC0::/42.

```
<Sysname> system-view
[Sysname] ipv6 prefix 3 88:99::/32
[Sysname] ipv6 dhcp prefix-pool 2 prefix 3 assign-len 42
```

Create prefix pool 1, and specify prefix 2001:0410::/32 with an assigned prefix length of 42. Prefix pool 1 contains 1024 prefixes from 2001:0410::/42 to 2001:0410:FFC0::/42.

```
<Sysname> system-view
[Sysname] ipv6 dhcp prefix-pool 1 prefix 2001:0410::/32 assign-len 42
```

Related commands

display ipv6 dhcp prefix-pool

prefix-pool

ipv6 dhcp server

Use **ipv6 dhcp server** to configure global address assignment on an interface. The server on the interface uses a global address pool to assign configuration information to a client.

Use **undo ipv6 dhcp server** to restore the default.

Syntax

ipv6 dhcp server { **allow-hint** | **preference** *preference-value* | **rapid-commit** } *

undo ipv6 dhcp server

Default

The server does not support desired address/prefix assignment or rapid address/prefix assignment. The server preference is set to 0.

Views

Interface view

Predefined user roles

network-admin

Parameters

allow-hint: Enables desired address/prefix assignment.

preference *preference-value*: Specifies the server preference in Advertise messages, in the range of 0 to 255. The default value is 0. A greater value represents a higher preference.

rapid-commit: Enables rapid address/prefix assignment involving two messages.

Usage guidelines

The **allow-hint** keyword enables the server to assign the desired address or prefix to the requesting client. If the desired address or prefix is not included in any global address pool, or is already assigned to another client, the server assigns the client a free address or a prefix. If the **allow-hint** keyword is not specified, the server ignores the desired address or prefix, and selects an address or prefix from a global address pool.

If you use the **ipv6 dhcp server** and **ipv6 dhcp server apply pool** commands on the same interface, the **ipv6 dhcp server apply pool** command takes effect.

Examples

Configure global address assignment on the interface VLAN-interface 2. Use the desired address/prefix assignment and rapid address/prefix assignment, and set the server preference to the highest 255.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ipv6 dhcp server allow-hint preference 255 rapid-commit
```

Related commands

display ipv6 dhcp server

ipv6 dhcp select

ipv6 dhcp server apply pool

Use **ipv6 dhcp server apply pool** to apply a DHCPv6 address pool to an interface.

Use **undo ipv6 dhcp server apply pool** to restore the default.

Syntax

ipv6 dhcp server apply pool *pool-name* [**allow-hint** | **preference** *preference-value* | **rapid-commit**] *

undo ipv6 dhcp server apply pool

Default

No DHCPv6 address pool is applied to an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

pool-name: Specifies a DHCPv6 address pool by its name, a case-insensitive string of 1 to 63 characters.

allow-hint: Enables desired address/prefix assignment.

preference *preference-value*: Specifies the server preference in Advertise messages, in the range of 0 to 255. The default value is 0. A greater value represents a higher preference.

rapid-commit: Enables rapid address/prefix assignment involving two messages.

Usage guidelines

Upon receiving a DHCPv6 request, the DHCPv6 server selects an IPv6 address or prefix from the address pool applied to the receiving interface. If no address pool is applied, the server selects an IPv6 address or prefix from a global address pool that matches the IPv6 address of the receiving interface or the DHCPv6 relay agent.

The **allow-hint** keyword enables the server to assign the desired address or prefix to the client. If the desired address or prefix does not exist or is already assigned to another client, the server assigns a free address or prefix. If **allow-hint** is not specified, the server ignores the desired address or prefix, and assigns a free address or prefix.

Only one address pool can be applied to an interface. If you execute this command multiple times, the most recent configuration takes effect.

A non-existing address pool can be applied to an interface, but the server cannot assign any prefix, address, or other configuration information from the address pool until the address pool is created.

Examples

Apply address pool 1 to VLAN-interface 2, configure the address pool to support desired address/prefix assignment and address/prefix rapid assignment, and set the preference to 255.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ipv6 dhcp server apply pool 1 allow-hint preference 255
rapid-commit
```

Related commands

display ipv6 dhcp server

ipv6 dhcp pool

ipv6 dhcp select

ipv6 dhcp server database filename

Use **ipv6 dhcp server database filename** to configure the DHCPv6 server to back up the DHCPv6 bindings to a file.

Use **undo ipv6 dhcp server database filename** to restore the default.

Syntax

ipv6 dhcp server database filename { *filename* | **url** *url* [**username** *username* [**password** { **cipher** | **simple** } *string*]] }

undo ipv6 dhcp server database filename

Default

The DHCPv6 server does not back up the DHCPv6 bindings.

Views

System view

Predefined user roles

network-admin

Parameters

filename: Specifies the name of a local backup file. For information about the *filename* argument, see *Fundamentals Configuration Guide*.

url *url*: Specifies the URL of a remote backup file. The URL is a case-sensitive string of 1 to 255 characters. Do not include a username or password in the URL.

username *username*: Specifies the username for accessing the URL of the remote backup file, a case-sensitive string of 1 to 32 characters. Do not specify this option if a username is not required for accessing the URL of the remote backup file.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 32 characters. Its encrypted form is a case-sensitive string of 1 to 73 characters. Do not specify this argument if a password is not required for accessing the URL of the remote backup file.

Usage guidelines

The command automatically creates the file if you specify a nonexistent file.

With this command executed, the DHCPv6 server backs up its bindings immediately and runs auto backup. The server, by default, waits 300 seconds after a binding change to update the backup file. You can use the **ipv6 dhcp server database update interval** command to change the waiting time. If no DHCPv6 binding changes, the backup file is not updated.

As a best practice, back up the bindings to a remote file. If you use the local storage medium, the frequent erasing and writing might damage the medium and then cause the DHCPv6 server to malfunction.

When the backup file is on a remote device, follow these restrictions and guidelines to specify the URL, username, and password:

- If the file is on an FTP server, enter URL in the format of ftp:*//server address:port/file path*, where the port number is optional.
- If the file is on a TFTP server, enter URL in the format of tftp:*//server address:port/file path*, where the port number is optional.
- The username and password must be the same as those configured on the FTP server. If the server authenticates only the username, the password can be omitted.
- If the IP address of the server is an IPv6 address, enclose the address in a pair of brackets, for example, **ftp://[1::1]/database.dhcp**.
- You can also specify the DNS domain name for the server address field, for example, **ftp://company/database.dhcp**.

Examples

Configure the DHCPv6 server to back up its bindings to the file **database.dhcp**

```
<Sysname> system-view
[Sysname] ipv6 dhcp server database filename database.dhcp
```

Configure the DHCPv6 server to back up its bindings to the file **database.dhcp** in the working directory of the FTP server at 10::1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp server database filename url ftp://[10::1]/database.dhcp username 1
password simple 1
```

Related commands

ipv6 dhcp server database update interval

ipv6 dhcp server database update now

ipv6 dhcp server database update stop

ipv6 dhcp server database update interval

Use **ipv6 dhcp server database update interval** to set the waiting time for the DHCPv6 server to update the backup file after a DHCPv6 binding change.

Use **undo ipv6 dhcp server database update interval** to restore the default.

Syntax

ipv6 dhcp server database update interval *interval*

undo ipv6 dhcp server database update interval

Default

The DHCPv6 server waits 300 seconds to update the backup file after a DHCPv6 binding change. If no DHCPv6 binding changes, the backup file is not updated.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Sets the waiting time in the range of 60 to 864000 seconds.

Usage guidelines

When a DHCPv6 binding is created, updated, or removed, the waiting period starts. The DHCPv6 server updates the backup file when the waiting period is reached. All bindings changed during the period will be saved to the backup file.

The waiting time takes effect only after you configure the DHCPv6 binding auto backup by using the **ipv6 dhcp server database filename** command.

Examples

Set the waiting time to 600 seconds for the DHCPv6 server to update the backup file.

```
<Sysname> system-view
[Sysname] ipv6 dhcp server database update interval 600
```

Related commands

ipv6 dhcp server database filename

ipv6 dhcp server database update now

ipv6 dhcp server database update stop

ipv6 dhcp server database update now

Use **ipv6 dhcp server database update now** to manually save the DHCPv6 bindings to the backup file.

Syntax

ipv6 dhcp server database update now

Views

System view

Predefined user roles

network-admin

Usage guidelines

Each time this command is executed, the DHCPv6 bindings are saved to the backup file.

For this command to take effect, you must configure the DHCPv6 auto backup by using the **ipv6 dhcp server database filename** command.

Examples

Manually save the DHCPv6 bindings to the backup file.

```
<Sysname> system-view
[Sysname] ipv6 dhcp server database update now
```

Related commands

ipv6 dhcp server database filename

ipv6 dhcp server database update interval

ipv6 dhcp server database update stop

ipv6 dhcp server database update stop

Use **ipv6 dhcp server database update stop** to terminate the download of DHCPv6 bindings from the backup file.

Syntax

ipv6 dhcp server database update stop

Views

System view

Predefined user roles

network-admin

Usage guidelines

The DHCPv6 server does not provide services during the binding download process. If the connection breaks up during the process, the waiting timeout timer is 60 minutes. When the timer expires, the DHCPv6 server stops waiting and starts providing address allocation services. You can execute this command to terminate the download immediately.

Manual termination allows the DHCPv6 server to provide services without waiting for the connection to be repaired. The IPv6 addresses and prefixes associated with the undownloaded bindings will be assigned to clients and address conflicts might occur.

Examples

Terminate the download of the backup DHCPv6 bindings.

```
<Sysname> system-view
[Sysname] ipv6 dhcp server database update stop
```

Related commands

ipv6 dhcp server database filename

ipv6 dhcp server database update interval

ipv6 dhcp server database update now

ipv6 dhcp server forbidden-address

Use **ipv6 dhcp server forbidden-address** to exclude IPv6 addresses in the DHCPv6 address pool from dynamic allocation.

Use **undo ipv6 dhcp server forbidden-address** to remove the configuration.

Syntax

ipv6 dhcp server forbidden-address *start-ipv6-address* [*end-ipv6-address*]

undo ipv6 dhcp server forbidden-address *start-ipv6-address* [*end-ipv6-address*]

Default

Except for the DHCPv6 server address, all IPv6 addresses in a DHCPv6 address pool are assignable.

Views

System view

Predefined user roles

network-admin

Parameters

start-ipv6-address: Specifies the start IPv6 address.

end-ipv6-address: Specifies the end IPv6 address, which cannot be lower than *start-ipv6-address*. If you do not specify an end IPv6 address, only the start IPv6 address is excluded from dynamic allocation. If you specify an end IPv6 address, the IP addresses from *start-ipv6-address* through *end-ipv6-address* are all excluded from dynamic allocation.

Usage guidelines

The IPv6 addresses of some devices such as the gateway and FTP server cannot be assigned to clients. Use this command to exclude such addresses from dynamic allocation.

If the excluded IPv6 address is in a static DHCPv6 binding, the address can still be assigned to the client.

The address or address range specified in the **undo** form of the command must be the same as the address or address range specified in the command. To remove an IP address that has been specified as part of an address range, you must remove the entire address range.

You can execute this command multiple times to exclude multiple IPv6 address ranges from dynamic allocation.

Examples

Exclude IPv6 addresses of 2001:10:110::1 through 2001:10:110::20 from dynamic assignment.

```
<Sysname> system-view
[Sysname] ipv6 dhcp server forbidden-address 2001:10:110::1 2001:10:110::20
```

Related commands

ipv6 dhcp server forbidden-prefix

static-bind

ipv6 dhcp server forbidden-prefix

Use **ipv6 dhcp server forbidden-prefix** to exclude IPv6 prefixes in the DHCPv6 prefix pool from dynamic allocation.

Use **undo ipv6 dhcp server forbidden-prefix** to remove the configuration.

Syntax

ipv6 dhcp server forbidden-prefix *start-prefix/prefix-len* [*end-prefix/prefix-len*]

undo ipv6 dhcp server forbidden-prefix *start-prefix/prefix-len* [*end-prefix/prefix-len*]

Default

No IPv6 prefixes in the DHCPv6 prefix pool are excluded from dynamic allocation.

Views

System view

Predefined user roles

network-admin

Parameters

start-prefix/prefix-len: Specifies the start IPv6 prefix. The *prefix-len* argument specifies the prefix length in the range of 1 to 128.

end-prefix/prefix-len: Specifies the end IPv6 prefix. The *prefix-len* argument specifies the prefix length in the range of 1 to 128. The value for *end-prefix* cannot be lower than that for *start-prefix*. If you do not specify this argument, only the *start-prefix/prefix-len* is excluded from dynamic allocation. If you specify this argument, the prefixes from *start-prefix/prefix-len* to *end-prefix/prefix-len* are all excluded.

Usage guidelines

If the excluded IPv6 prefix is in a static binding, the prefix can still be assigned to the client.

The prefix or prefix range specified in the **undo** form of the command must be the same as the prefix or prefix range specified in the command. To remove a prefix that has been specified as part of a prefix range, you must remove the entire prefix range.

You can execute this command multiple times to exclude multiple IPv6 prefix ranges from dynamic allocation.

Examples

Exclude IPv6 prefixes from 2001:3e11::/32 through 2001:3eff::/32 from dynamic allocation.

```
<Sysname> system-view
[Sysname] ipv6 dhcp server forbidden-prefix 2001:3e11::/32 2001:3eff::/32
```

Related commands

ipv6 dhcp server forbidden-address

static-bind

network

Use **network** to specify an IPv6 subnet for dynamic allocation in a DHCPv6 address pool.

Use **undo network** to restore the default.

Syntax

network { *prefix/prefix-length* | **prefix** *prefix-number* [*sub-prefix/sub-prefix-length*] } [**preferred-lifetime** *preferred-lifetime* **valid-lifetime** *valid-lifetime*]

undo network

Default

No IPv6 subnet is specified in a DHCPv6 address pool.

Views

DHCPv6 address pool view

Predefined user roles

network-admin

Parameters

prefix/prefix-length: Specifies the IPv6 subnet for dynamic allocation. The value range for the *prefix-length* argument is 1 to 128.

prefix *prefix-number*: Specifies an IPv6 prefix by its ID in the range of 1 to 1024.

sub-prefix/*sub-prefix-length*: Specifies an IPv6 sub-prefix and its length. The value range for the *sub-prefix-length* argument is 1 to 128. If the IPv6 prefix is longer than the IPv6 sub-prefix or if you do not specify an IPv6 sub-prefix, the IPv6 subnet defined by the IPv6 prefix is used for dynamic allocation.

preferred-lifetime *preferred-lifetime*: Sets the preferred lifetime. The value range is 60 to 4294967295 seconds, and the default is 604800 seconds (7 days).

valid-lifetime *valid-lifetime*: Sets the valid lifetime. The value range is 60 to 4294967295 seconds, and the default is 2592000 seconds (30 days). The valid lifetime must be longer than or equal to the preferred lifetime.

Usage guidelines

You can specify only one subnet for a DHCPv6 address pool. If you execute the **network** command multiple times, the most recent configuration takes effect.

Modifying or removing the **network** command configuration removes assigned addresses in the current address pool.

The **network prefix** command does not take effect if the specified IPv6 prefix does not exist. This command takes effect after the IPv6 prefix is created.

The **network** command defines the IPv6 subnet for dynamic allocation through the *prefix/prefix-length* arguments or the *prefix-number* [*sub-prefix*/*sub-prefix-length*] arguments. The IPv6 subnets cannot be the same in different DHCPv6 address pools.

If the prefix that the ID represents is changed, the IPv6 subnet in this command accordingly changes, and the assigned prefix and address bindings are cleared.

Examples

Specify the subnet 3ffe:501:ffff:100::/64 in DHCPv6 address pool 1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] network 3ffe:501:ffff:100::/64
```

Create IPv6 prefix 88:99::/32 with the prefix ID 3. Create DHCPv6 address pool 1 and use the IPv6 subnet defined by the IPv6 prefix for dynamic allocation.

```
<Sysname> system-view
[Sysname] ipv6 prefix 3 88:99::/32
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] network prefix 3
```

Create IPv6 prefix 88:99::/32 with the prefix ID 3. Create DHCPv6 address pool 1 and use IPv6 subnet 88:99:ffff:100::/64 defined by IPv6 prefix 3 and IPv6 sub-prefix 3ffe:501:ffff:100::/64 for dynamic allocation. The first 32 bits of the IPv6 subnet are determined by IPv6 prefix 3. The bits 33 to 64 of the IPv6 subnet are determined by the IPv6 sub-prefix and its length. The prefix length of the IPv6 subnet is the IPv6 sub-prefix length.

```
<Sysname> system-view
[Sysname] ipv6 prefix 3 88:99::/32
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] network prefix 3 3ffe:501:ffff:100::/64
```

Related commands

address range

display ipv6 dhcp pool

temporary address range

option

Use **option** to configure a self-defined DHCPv6 option in a DHCPv6 address pool.

Use **undo option** to remove a self-defined DHCPv6 option from a DHCPv6 address pool.

Syntax

option *code* **hex** *hex-string*

undo option *code*

Default

No self-defined DHCPv6 option is configured in a DHCPv6 address pool.

Views

DHCPv6 address pool view

DHCPv6 option group view

Predefined user roles

network-admin

Parameters

code: Specifies a number for the self-defined option, in the range of 21 to 65535, excluding 25 through 26, 37 through 40, and 43 through 48.

hex *hex-string*: Specifies the content of the option, a hexadecimal number whose length is an even number in the range of 2 to 256.

Usage guidelines

The DHCPv6 server fills the self-defined option with the specified hexadecimal number and sends it in a response to the client.

You can self-define options for the following purposes:

- Add newly released options.
- Add options for which the vendor defines the contents, for example, Option 43.

- Add options for which the CLI does not provide a dedicated configuration command like **dns-server**. For example, you can use the **option 31 hex 0200000000000000000000000000001** command to define the NTP server address 200::1 for DHCP clients.

If a DHCPv6 option is specified by both the dedicated command and the **option** command, the DHCPv6 server preferentially assigns the content specified by the dedicated command. For example, if a DNS server address is specified by the **dns-server** command and the **option 23** command, the server uses the address specified by **dns-server** command.

If you execute this command multiple times with the same *code* specified, the most recent configuration takes effect.

Examples

Configure Option 23 that specifies a DNS server address 2001:f3e0::1 in DHCPv6 address pool 1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] option 23 hex 2001f3e000000000000000000000001
```

Related commands

display ipv6 dhcp pool

dns-server

domain-name

sip-server

option-group

Use **option-group** to specify a DHCPv6 option group for a DHCPv6 address pool.

Use **undo option-group** to restore the default.

Syntax

option-group *option-group-number*

undo option-group

Default

No DHCPv6 option group is specified for a DHCPv6 address pool.

Views

DHCPv6 address pool view

Predefined user roles

network-admin

Parameters

option-group--number: Specifies a DHCPv6 option group by its number in the range of 1 to 100.

Examples

Specify DHCPv6 option group 1 for DHCPv6 address pool 1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] option-group 1
```

Related commands

display ipv6 dhcp pool

ipv6 dhcp option-group

prefix-pool

Use **prefix-pool** to apply a prefix pool to a DHCPv6 address pool, so the DHCPv6 server can dynamically select a prefix from the prefix pool for a client.

Use **undo prefix-pool** to remove the prefix pool.

Syntax

prefix-pool *prefix-pool-number* [**preferred-lifetime** *preferred-lifetime* **valid-lifetime** *valid-lifetime*]

undo prefix-pool *prefix-pool-number*

Default

No prefix pool is applied to a DHCPv6 address pool.

Views

DHCPv6 address pool view

Predefined user roles

network-admin

Parameters

prefix-pool-number: Specifies a prefix pool by its number in the range of 1 to 128.

preferred-lifetime *preferred-lifetime*: Sets the preferred lifetime in the range of 60 to 4294967295 seconds. The default value is 604800 seconds (7 days).

valid-lifetime *valid-lifetime*: Sets the valid lifetime in the range of 60 to 4294967295 seconds. The default value is 2592000 seconds (30 days). The valid lifetime must be longer than or equal to the preferred lifetime.

Usage guidelines

Only one prefix pool can be applied to an address pool.

You can apply a prefix pool that has not been created to an address pool. The setting takes effect after the prefix pool is created.

To modify the prefix pool in a DHCPv6 address pool, execute the **undo prefix-pool** command to remove the prefix pool, and then execute the **prefix-pool** command.

Examples

Apply prefix pool 1 to address pool 1, and use the default preferred lifetime and valid lifetime.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] prefix-pool 1
```

Apply prefix pool 2 to address pool 2, and set the preferred lifetime to one day and the valid lifetime to three days.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 2
[Sysname-dhcp6-pool-2] prefix-pool 2 preferred-lifetime 86400 valid-lifetime 259200
```

Related commands

display ipv6 dhcp pool

ipv6 dhcp prefix-pool

reset ipv6 dhcp server conflict

Use **reset ipv6 dhcp server conflict** to clear IPv6 address conflict information.

Syntax

reset ipv6 dhcp server conflict [**address** *ipv6-address*]

Views

User view

Predefined user roles

network-admin

Parameters

address *ipv6-address*: Clears conflict information for the specified IPv6 address. If you do not specify an IPv6 address, this command clears all IPv6 address conflict information.

Usage guidelines

Address conflicts occur when dynamically assigned IP addresses have been statically configured for other hosts. After the conflicts are resolved, you can use the **reset ipv6 dhcp server conflict** command to clear conflict information so that the conflicted addresses can be assigned to clients.

Examples

Clear all IPv6 address conflict information.

```
<Sysname> reset ipv6 dhcp server conflict
```

Related commands

display ipv6 dhcp server conflict

reset ipv6 dhcp server expired

Use **reset ipv6 dhcp server expired** to clear binding information for lease-expired IPv6 addresses.

Syntax

reset ipv6 dhcp server expired [**address** *ipv6-address* | **pool** *pool-name*]

Views

User view

Predefined user roles

network-admin

Parameters

address *ipv6-address*: Clears binding information for the specified lease-expired IPv6 address. If you do not specify an IPv6 address, this command clears binding information for all lease-expired IPv6 address.

pool *pool-name*: Clears binding information for lease-expired IPv6 addresses in the address pool specified by its name, a case-insensitive string of 1 to 63 characters. If you do not specify an address pool, this command clears binding information for lease-expired IPv6 addresses in all address pools.

Examples

Clear binding information for expired IPv6 address 2001:f3e0::1.

```
<Sysname> reset ipv6 dhcp server expired address 2001:f3e0::1
```

Related commands

display ipv6 dhcp server expired

reset ipv6 dhcp server ip-in-use

Use **reset ipv6 dhcp server ip-in-use** to clear binding information for assigned IPv6 addresses.

Syntax

reset ipv6 dhcp server ip-in-use [**address** *ipv6-address* | **pool** *pool-name*]

Views

User view

Predefined user roles

network-admin

Parameters

address *ipv6-address*: Clears binding information for the specified assigned IPv6 address. If you do not specify an IPv6 address, this command clears binding information for all assigned IPv6 addresses.

pool *pool-name*: Clears binding information for assigned IPv6 addresses in the address pool specified by its name, a case-insensitive string of 1 to 63 characters. If you do not specify an address pool, this command clears binding information for assigned IPv6 addresses in all address pools.

Usage guidelines

If you execute this command to clear information about an assigned static binding, the static binding becomes a free static binding.

Examples

Clear binding information for all assigned IPv6 addresses.

```
<Sysname> reset ipv6 dhcp server ip-in-use
```

Clears binding information for assigned IPv6 addresses in DHCPv6 address pool 1.

```
<Sysname> reset ipv6 dhcp server ip-in-use pool 1
```

Clears binding information for the assigned IPv6 address 2001:0:0:1::1.

```
<Sysname> reset ipv6 dhcp server ip-in-use address 2001:0:0:1::1
```

Related commands

display ipv6 dhcp server ip-in-use

reset ipv6 dhcp server pd-in-use

Use **reset ipv6 dhcp server pd-in-use** to clear binding information for assigned IPv6 prefixes.

Syntax

reset ipv6 dhcp server pd-in-use [**pool** *pool-name* | **prefix** *prefix/prefix-len*]

Views

User view

Predefined user roles

network-admin

Parameters

pool *pool-name*: Clears binding information for assigned IPv6 prefixes in the address pool specified by its name, a case-insensitive string of 1 to 63 characters. If you do not specify an address pool, this command clears binding information for assigned IPv6 prefixes in all address pools.

prefix *prefix/prefix-len*: Clears binding information for the specified assigned IPv6 prefix. The value range for the prefix length is 1 to 128. If you do not specify an IPv6 prefix, this command clears binding information for all assigned IPv6 prefixes.

Usage guidelines

If you execute this command to clear information about an assigned static binding, the static binding becomes a free static binding.

Examples

Clear binding information for all assigned IPv6 prefixes.

```
<Sysname> reset ipv6 dhcp server pd-in-use
```

Clears binding information for assigned IPv6 prefixes in DHCPv6 address pool 1.

```
<Sysname> reset ipv6 dhcp server pd-in-use pool 1
```

Clears binding information for the assigned IPv6 prefix 2001:0:0:1::/64.

```
<Sysname> reset ipv6 dhcp server pd-in-use prefix 2001:0:0:1::/64
```

Related commands

display ipv6 dhcp server pd-in-use

reset ipv6 dhcp server statistics

Use **reset ipv6 dhcp server statistics** to clear DHCPv6 server statistics.

Syntax

reset ipv6 dhcp server statistics

Views

User view

Predefined user roles

network-admin

Examples

Clear DHCPv6 server statistics.

```
<Sysname> reset ipv6 dhcp server statistics
```

Related commands

display ipv6 dhcp server statistics

sip-server

Use **sip-server** to specify the IPv6 address or domain name of a SIP server in the DHCPv6 address pool.

Use **undo sip-server** to remove a SIP server.

Syntax

sip-server { **address** *ipv6-address* | **domain-name** *domain-name* }

undo sip-server { **address** *ipv6-address* | **domain-name** *domain-name* }

Default

No SIP server address or domain name is specified.

Views

DHCPv6 address pool view

DHCPv6 option group view

Predefined user roles

network-admin

Parameters

address *ipv6-address*: Specifies the IPv6 address of a SIP server.

domain-name *domain-name*: Specifies the domain name of a SIP server, a case-insensitive string of 1 to 50 characters.

Usage guidelines

You can specify up to eight SIP server addresses and eight SIP server domain names in an address pool. A SIP server that is specified earlier has a higher preference.

Examples

Specify the SIP server address **2:2::4** in DHCPv6 address pool 1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] sip-server address 2:2::4
```

Specify the SIP server domain name **bbb.com** in DHCPv6 address pool 1.

```
[Sysname-dhcp6-pool-1] sip-server domain-name bbb.com
```

Related commands

display ipv6 dhcp pool

static-bind

Use **static-bind** to statically bind an IPv6 address or prefix to a client in the DHCPv6 address pool.

Use **undo static-bind** to delete a static binding.

Syntax

static-bind { **address** *ipv6-address*/*addr-prefix-length* | **prefix** *prefix*/*prefix-len* } **duid** *duid* [**iaid** *iaid*] [**preferred-lifetime** *preferred-lifetime* **valid-lifetime** *valid-lifetime*]

undo static-bind { **address** *ipv6-address*/*addr-prefix-length* | **prefix** *prefix*/*prefix-len* }

Default

No static binding is configured in a DHCPv6 address pool.

Views

DHCPv6 address pool view

Predefined user roles

network-admin

Parameters

address *ipv6-address*/*addr-prefix-length*: Specifies the IPv6 address and prefix length. The value range for the prefix length is 1 to 128.

prefix *prefix*/*prefix-len*: Specifies the prefix and prefix length. The value range for the prefix length is 1 to 128.

duid *duid*: Specifies a client DUID. The value is an even hexadecimal number in the range of 2 to 256.

iaid *iaid*: Specifies a client IAID. The value is a hexadecimal number in the range of 0 to FFFFFFFF. If you do not specify an IAID, the server does not match the client IAID for prefix assignment.

preferred-lifetime *preferred-lifetime*: Sets the preferred lifetime of the address or prefix. The value range is 60 to 4294967295 seconds, and the default is 604800 seconds (7 days).

valid-lifetime *valid-lifetime*: Sets the valid lifetime of the address or prefix. The value range is 60 to 4294967295 seconds, and the default is 2592000 seconds (30 days). The valid lifetime cannot be shorter than the preferred lifetime.

Usage guidelines

You can specify multiple static bindings in a DHCPv6 address pool.

An IPv6 address or prefix can be bound to only one DHCPv6 client.

To modify a static binding, execute the **undo static-bind** command to delete the binding, and then execute the **static-bind** command.

Examples

In address pool 1, bind IPv6 address 2001:0410::/35 to the client DUID 0003000100e0fc005552 and IAID A1A1A1A1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] static-bind address 2001:0410::/35 duid 0003000100e0fc005552 iaid A1A1A1A1
```

In address pool 1, bind prefix 2001:0410::/35 to the client DUID 00030001CA0006A400 and IAID A1A1A1A1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] static-bind prefix 2001:0410::/35 duid 00030001CA0006A400 iaid A1A1A1A1
```

Related commands

display ipv6 dhcp pool

temporary address range

Use **temporary address range** to configure a temporary IPv6 address range in a DHCPv6 address pool for dynamic allocation.

Use **undo temporary address range** to restore the default.

Syntax

temporary address range *start-ipv6-address end-ipv6-address* [**preferred-lifetime** *preferred-lifetime* **valid-lifetime** *valid-lifetime*]

undo temporary address range

Default

No temporary IPv6 address range is configured in a DHCPv6 address pool.

Views

DHCPv6 address pool view

Predefined user roles

network-admin

Parameters

start-ipv6-address: Specifies the start IPv6 address.

end-ipv6-address: Specifies the end IPv6 address.

preferred-lifetime *preferred-lifetime*: Sets the preferred lifetime. The value range is 60 to 4294967295 seconds, and the default is 604800 seconds (7 days).

valid-lifetime *valid-lifetime*: Sets the valid lifetime. The value range is 60 to 4294967295 seconds, and the default is 2592000 seconds (30 days). The valid lifetime cannot be shorter than the preferred lifetime.

Usage guidelines

If you do not execute the **temporary address range** command, the DHCPv6 server does not support temporary address assignment.

You can configure only one temporary IPv6 address range in an address pool. If you execute this command multiple times, the most recent configuration takes effect.

Examples

In DHCPv6 address pool 1, configure a temporary IPv6 address range from 3ffe:501:ffff:100::50 to 3ffe:501:ffff:100::60.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] network 3ffe:501:ffff:100::/64
[Sysname-dhcp6-pool-1] temporary address range 3ffe:501:ffff:100::50
3ffe:501:ffff:100::60
```

Related commands

display ipv6 dhcp pool

address range

network

DHCPv6 relay agent commands

display ipv6 dhcp relay server-address

Use **display ipv6 dhcp relay server-address** to display DHCPv6 server addresses specified on the DHCPv6 relay agent.

Syntax

display ipv6 dhcp relay server-address [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays DHCPv6 server addresses on all interfaces enabled with DHCPv6 relay agent.

Examples

Display DHCPv6 server addresses on all interfaces enabled with DHCPv6 relay agent.

```
<Sysname> display ipv6 dhcp relay server-address
Interface: Vlan-interface2
 Server address     Outgoing Interface          Public/VRF name
 2::3                                           --/--
 3::4               Vlan-interface4             Y/--
 4::5                                           --/1

Interface: Vlan-interface3
 Server address     Outgoing Interface          Public/VRF name
 2::3                                           --/--
 3::4               Vlan-interface4             Y/--
 4::5                                           --/1
```

Display DHCPv6 server addresses on VLAN-interface 2.

```
<Sysname> display ipv6 dhcp relay server-address interface vlan-interface 2
Interface: Vlan-interface2
 Server address     Outgoing Interface          Public/VRF name
 2::3                                           --/--
 3::4               Vlan-interface4             Y/--
 4::5                                           --/1
```

Table 11 Command output

Field	Description
Server address	DHCPv6 server address specified on the DHCP relay agent.

Field	Description
Outgoing Interface	Output interface of DHCPv6 packets. If no output interface is specified, the device searches the routing table for the output interface.
Public/VRF name	This field is not supported in the current software version. Location of the DHCPv6 server, which is determined by the configuration of the **ipv6 dhcp relay server-address** command. • If neither the **public** keyword nor the **vpn-instance** *vpn-instance-name* option is specified, this field displays **--/--**. • If the **public** keyword is specified, this field displays **Y/--**. • If the **vpn-instance** *vpn-instance-name* option is specified, the VPN instance name is displayed after the slash (/), for example, **--/1**.

Related commands

ipv6 dhcp relay server-address

ipv6 dhcp select

display ipv6 dhcp relay statistics

Use **display ipv6 dhcp relay statistics** to display DHCPv6 packet statistics on the DHCPv6 relay agent.

Syntax

display ipv6 dhcp relay statistics [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays DHCPv6 packets statistics on all interfaces enabled with DHCPv6 relay agent.

Examples

Display DHCPv6 packet statistics on all interfaces enabled with DHCPv6 relay agent.

```
<Sysname> display ipv6 dhcp relay statistics
Packets dropped               :  4
Packets received              :  14
    Solicit                   :  0
    Request                   :  0
    Confirm                   :  0
    Renew                     :  0
    Rebind                    :  0
    Release                   :  0
```

```
    Decline                  :  0
    Information-request      :  7
    Relay-forward            :  0
    Relay-reply              :  7
Packets sent                 :  14
    Advertise                :  0
    Reconfigure              :  0
    Reply                    :  7
    Relay-forward            :  7
    Relay-reply              :  0
```

Display DHCPv6 packet statistics on the DHCPv6 relay agent on VLAN-interface 2.

```
<Sysname> display ipv6 dhcp relay statistics interface vlan-interface 2
Packets dropped              :  4
Packets received             :  16
    Solicit                  :  0
    Request                  :  0
    Confirm                  :  0
    Renew                    :  0
    Rebind                   :  0
    Release                  :  0
    Decline                  :  0
    Information-request      :  8
    Relay-forward            :  0
    Relay-reply              :  8
Packets sent                 :  16
    Advertise                :  0
    Reconfigure              :  0
    Reply                    :  8
    Relay-forward            :  8
    Relay-reply              :  0
```

Table 12 Command output

Field	Description
Packets dropped	Number of discarded packets.
Packets received	Number of received packets.
Solicit	Number of received solicit packets.
Request	Number of received request packets.
Confirm	Number of received confirm packets.
Renew	Number of received renew packets.
Rebind	Number of received rebind packets.
Release	Number of received release packets.
Decline	Number of received decline packets.
Information-request	Number of received information request packets.
Relay-forward	Number of received relay-forward packets.
Relay-reply	Number of received relay-reply packets.

Field	Description
Packets sent	Number of sent packets.
Advertise	Number of sent advertise packets.
Reconfigure	Number of sent reconfigure packets.
Reply	Number of sent reply packets.
Relay-forward	Number of sent Relay-forward packets.
Relay-reply	Number of sent Relay-reply packets.

Related commands

reset ipv6 dhcp relay statistics

gateway-list

Use **gateway-list** to specify gateway addresses for DHCPv6 clients in a DHCPv6 address pool.

Use **undo gateway-list** to remove gateway addresses from a DHCPv6 address pool.

Syntax

gateway-list *ipv6-address*&<1-8>

undo gateway-list [*ipv6-address*&<1-8>]

Default

No gateway address is specified in a DHCPv6 address pool.

Views

DHCPv6 address pool view

Predefined user roles

network-admin

Parameters

ipv6-address&<1-8>: Specifies a space-separated list of up to eight addresses.

Usage guidelines

DHCPv6 clients of the same access type can be classified into different types by their locations. In this case, the relay interface typically has no IPv6 address configured. You can use the **gateway-list** command to specify gateway addresses for clients matching the same DHCPv6 address pool.

Upon receiving a DHCPv6 Solicit or Request from a client that matches a DHCPv6 address pool, the relay agent processes the packet as follows:

- Fills the **link-address** field of the packet with a specified gateway address.
- Forwards the packet to all DHCPv6 servers in the matching DHCPv6 address pool.

The DHCPv6 servers select a DHCPv6 address pool according to the gateway address.

Examples

Specify the gateway address 10::1 in the DHCPv6 address pool **p1**.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool p1
[Sysname-dhcp6-pool-p1] gateway-list 10::1
```

ipv6 dhcp advertise address-route

Use **ipv6 dhcp advertise address-route** to enable the DHCPv6 relay agent to advertise host routes for IPv6 addresses assigned to DHCP clients.

Use **undo ipv6 dhcp advertise address-route** to disable the DHCPv6 relay agent from advertising host routes for IPv6 addresses assigned to DHCPv6 clients.

Syntax

ipv6 dhcp advertise address-route

undo ipv6 dhcp advertise address-route

Default

The DHCPv6 relay agent does not advertise host routes for IPv6 addresses assigned to DHCPv6 clients.

Views

System view

Predefined user roles

network-admin

Usage guidelines

In a network where ND cannot resolve global unicast addresses, network devices cannot generate ND entries for all global unicast addresses. If a DHCPv6 client obtains a global unicast address, the neighboring devices do not have the ND entries for this global unicast address, thus cannot forward the packets destined for the client. To resolve this problem, enable the DHCPv6 relay agent to advertise host routes for assigned IPv6 addresses in DHCP replies. The advertised route information is as follows:

- The destination IP address is the assigned IPv6 address.
- The next hop is the link-local address of the DHCPv6 client.
- The output interface is the interface that forwards the reply.

After the relay agent receives a packet destined for the assigned IPv6 address, the relay agent looks up the routing table for the next hop. ND resolution can succeed because the next hop is the link-local address of the client. The relay agent searches the ND table for the MAC address of the client based on the next hop and then forwards the packet.

Before using this command on the DHCPv6 relay agent, enable the DHCPv6 relay agent to record DHCPv6 relay entries first.

Examples

Enable the DHCPv6 relay agent to advertise host routes for IPv6 addresses assigned to DHCPv6 clients.

```
<Sysname> system-view
[Sysname] ipv6 dhcp advertise address-route
```

Related commands

ipv6 dhcp relay client-information record

ipv6 dhcp relay client-link-address enable

Use **ipv6 dhcp relay client-link-address enable** to enable the DHCPv6 relay agent to support Option 79.

Use **undo ipv6 dhcp relay client-link-address enable** to disable Option 79 support.

Syntax

ipv6 dhcp relay client-link-address enable

undo ipv6 dhcp relay client-link-address enable

Default

The DHCPv6 relay agent does not support Option 79.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

If DHCPv6 relay agents exist in the network, the DHCPv6 server needs the MAC address of the DHCPv6 client for authentication or for IPv6 address or prefix assignment. To meet the requirement, enable the DHCPv6 relay agent that the client first passes to support Option 79. This feature allows the DHCPv6 relay agent to learn the MAC address in the client request. When the relay agent generates a Relay-Forward packet for the request, it fills the MAC address of the client in Option 79. The Relay-Forward packet is then forwarded to the DHCPv6 server.

Examples

Enable Option 79 support on the relay agent.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ipv6 dhcp relay client-link-address enable
```

ipv6 dhcp relay gateway

Use **ipv6 dhcp relay gateway** to specify a gateway address for DHCPv6 clients on the DHCPv6 relay interface.

Use **undo ipv6 dhcp relay gateway** to restore the default.

Syntax

ipv6 dhcp relay gateway *ipv6-address*

undo ipv6 dhcp relay gateway

Default

The first IPv6 address of the relay interface is used as the gateway address for DHCPv6 clients.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies a gateway address. The IPv6 address must be an IPv6 address of the relay interface.

Usage guidelines

The DHCPv6 relay agent uses the specified IPv6 address instead of the first IPv6 address of the relay interface as the gateway address for DHCPv6 clients.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify 10::1 as the gateway address for DHCPv6 clients on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ipv6 dhcp relay gateway 10::1
```

Related commands

gateway-list

ipv6 dhcp relay interface-id

Use **ipv6 dhcp relay interface-id** to specify a padding mode for the Interface-ID option.

Use **undo ipv6 dhcp relay interface-id** to restore the default.

Syntax

ipv6 dhcp relay interface-id { **bas** | **interface** }

undo ipv6 dhcp relay interface-id

Default

The DHCPv6 relay agent fills the Interface-ID option with the interface index of the interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

bas: Specifies the BAS mode.

interface: Specifies the interface name mode. This mode pads the Interface-ID option in ASCII code with the interface name and VLAN ID of the interface.

Usage guidelines

Enable the DHCPv6 relay agent on the interface before executing this command. Otherwise, the command does not take effect.

Examples

Specify the BAS mode as the padding mode for the Interface-ID option on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ipv6 dhcp relay interface-id bas
```

Specify the interface name mode as the padding mode for the Interface-ID option on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ipv6 dhcp relay interface-id interface
```

ipv6 dhcp relay server-address

Use **ipv6 dhcp relay server-address** to specify a DHCPv6 server on the DHCPv6 relay agent.

Use **undo ipv6 dhcp relay server-address** to remove DHCPv6 server addresses.

Syntax

ipv6 dhcp relay server-address *ipv6-address* [**interface** *interface-type interface-number*]

undo ipv6 dhcp relay server-address [*ipv6-address* [**interface** *interface-type interface-number*]]

Default

No DHCPv6 server address is specified on the DHCPv6 relay agent.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the IPv6 address of a DHCPv6 server.

interface *interface-type interface-number*: Specifies an output interface through which the relay agent forwards the DHCPv6 requests to the DHCPv6 server. If you do not specify an output interface, the relay agent looks up the routing table for an output interface.

Usage guidelines

Upon receiving a request from a DHCPv6 client, the interface encapsulates the request into a Relay-forward message and forwards the message to the specified DHCPv6 server.

You can specify a maximum of eight DHCPv6 servers on an interface. The DHCPv6 relay agent forwards DHCP requests to all the specified DHCPv6 servers.

If the DHCPv6 server address is a link-local address or multicast address, you must specify an output interface. If you do not specify an output interface, DHCPv6 packets might fail to reach the DHCPv6 server.

If you do not specify an IPv6 address, the **undo ipv6 dhcp relay server-address** command removes all DHCPv6 server addresses specified on the interface.

Do not enable the DHCPv6 client and the DHCPv6 relay agent on the same interface.

Examples

Enable the DHCPv6 relay agent on VLAN-interface 2 and specify the DHCPv6 server address 2001:1::3.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ipv6 dhcp select relay
[Sysname-Vlan-interface2] ipv6 dhcp relay server-address 2001:1::3
```

Related commands

display ipv6 dhcp relay server-address

ipv6 dhcp select

ipv6 dhcp relay source-address

Use **ipv6 dhcp relay source-address** to specify the source IPv6 address for relayed DHCPv6 requests.

Use **undo ipv6 dhcp relay source-address** to restore the default.

Syntax

ipv6 dhcp relay source-address { *ipv6-address* | **interface** *interface-type interface-number* }

undo ipv6 dhcp relay source-address

Default

The DHCPv6 relay agent uses the IPv6 global unicast address of the interface that connects to the DHCPv6 server as the source IPv6 address for relayed DHCPv6 requests.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies a source IPv6 address.

interface *interface-type interface-number*: Uses the IPv6 address of an interface as the source IPv6 address. The *interface-type interface-number* arguments specify an interface by its type and number.

Usage guidelines

This command is required if a relay interface does not have routes to DHCPv6 servers. You can specify a global unicast address or the IPv6 address of another interface (typically the loopback interface) as the source IPv6 address for DHCPv6 requests. The relay interface inserts the source IPv6 address in the source IPv6 address field of DHCPv6 requests.

If the specified interface does not have a global unicast IPv6 address, the IPv6 address of the output interface is used as the source address for relayed DHCPv6 requests.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify 10::1 as the source IPv6 address for relayed DHCPv6 requests on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ipv6 dhcp relay source-address 10::1
```

remote-server

Use **remote-server** to specify DHCPv6 servers for a DHCPv6 address pool.

Use **undo remote-server** to remove DHCPv6 servers from a DHCPv6 address pool.

Syntax

remote-server *ipv6-address* [**interface** *interface-type interface-number*]

undo remote-server [*ipv6-address* [**interface** *interface-type interface-number*]]

Default

No DHCPv6 server is specified for the DHCPv6 address pool.

Views

DHCPv6 address pool view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies a DHCPv6 server address.

interface *interface-type interface-number*: Specifies the outgoing interface by its type and number for the DHCPv6 relay agent to forward packets to the DHCPv6 server. If you do not specify an outgoing interface, the DHCPv6 relay agent performs a routing table lookup.

Usage guidelines

You can specify a maximum of eight DHCPv6 servers in one DHCPv6 address pool.

If you do not specify any parameters, the **undo remote-server** command removes all DHCPv6 servers in the DHCPv6 address pool.

If a DHCPv6 server address is a link-local address, you must specify an outgoing interface by using the **interface** keyword in this command. If you do not specify an outgoing interface, DHCPv6 packets might fail to reach the DHCPv6 server.

Examples

Specify DHCPv6 server 10::1 for DHCPv6 address pool 0.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 0
[Sysname-dhcp6-pool-0] remote-server 10::1
```

reset ipv6 dhcp relay statistics

Use **reset ipv6 dhcp relay statistics** to clear packets statistics on the DHCPv6 relay agent.

Syntax

reset ipv6 dhcp relay statistics [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command clears all relay agent statistics.

Examples

Clear packet statistics on the DHCPv6 relay agent.

```
<Sysname> reset ipv6 dhcp relay statistics
```

Related commands

display ipv6 dhcp relay statistics

DHCPv6 client commands

display ipv6 dhcp client

Use **display ipv6 dhcp client** to display DHCPv6 client information.

Syntax

display ipv6 dhcp client [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays information about all DHCPv6 clients.

Examples

Display the DHCPv6 client information on VLAN-interface 2.

```
<Sysname> display ipv6 dhcp client interface vlan-interface 2
Vlan-interface2:
  Type: Stateful client requesting address and prefix
    State: OPEN
    Client DUID: 0003000100e002000000
    Preferred server:
      Reachable via address: FE80::2E0:1FF:FE00:18
      Server DUID: 0003000100e001000000
    IA_NA: IAID 0x00000642, T1 50 sec, T2 80 sec
      Address: 1:1::2/128
        Preferred lifetime 100 sec, valid lifetime 200 sec
        Will expire on Feb 4 2014 at 15:37:20(288 seconds left)
    IA_PD: IAID 0x00000642, T1 50 sec, T2 80 sec
      Prefix: 12:34::/48
        Preferred lifetime 100 sec, valid lifetime 200 sec
        Will expire on Mar 27 2014 at 08:13:24 (199 seconds left)
    DNS server addresses:
      2:2::3
    Domain name:
      aaa.com
    SIP server addresses:
      2:2::4
    SIP server domain names:
      bbb.com
```

```
Options:
  Code: 88
    Length: 3 bytes
    Hex: AABBCC
```

Table 13 Command output

Field	Description
Type	Types of DHCPv6 client: • **Stateful client requesting address**—A DHCPv6 client that requests an IPv6 address. • **Stateful client requesting prefix**—A DHCPv6 client that requests an IPv6 prefix. • **Stateful client requesting address and prefix**—A DHCPv6 client that requests an IPv6 address and prefix. • **Stateless client**—A DHCPv6 client that requests configuration parameters other than an IPv6 address and prefix through stateless DHCPv6.
State	Current state of the DHCPv6 client: • **IDLE**—The client is in idle state. • **SOLICIT**—The client is locating a DHCPv6 server. • **REQUEST**—The client is requesting an IPv6 address or prefix. • **OPEN**—The client has obtained an IPv6 address or prefix. • **RENEW**—The client is extending the lease (after T1 and before T2). • **REBIND**—The client is extending the lease (after T2 and before the lease expires). • **RELEASE**—The client is releasing an IPv6 address or prefix. • **DECLINE**—The client is declining an IPv6 address or prefix because of an address or prefix conflict. • **INFO-REQUESTING**—The client is requesting configuration parameters through stateless DHCPv6.
Client DUID	DUID of the DHCPv6 client.
Preferred server	Information about the DHCPv6 server selected by the DHCPv6 client.
Reachable via address	Reachable address for the DHCPv6 client. It is the link local address of the DHCPv6 server or DHCPv6 relay agent.
Server DUID	DUID of the DHCPv6 server.
IA_NA	IA_NA information.
IA_PD	IA_PD information.
IAID	IA identifier.
T1	T1 value in seconds.
T2	T2 value in seconds.
Address	IPv6 address obtained. This field is displayed only when the DHCPv6 client type is **Stateful client requesting address**.
Prefix	IPv6 prefix obtained. This field is displayed only when the DHCPv6 client type is **Stateful client requesting prefix**.
Preferred lifetime	Preferred lifetime in seconds.
valid lifetime	Valid lifetime in seconds.

Field	Description
Will expire on Feb 4 2014 at 15:37:20 (288 seconds left)	Time when the lease expires and the remaining time of the lease. If the lease expires after the year 2100, this field displays **Will expire after 2100**.
DNS server addresses	IPv6 address of the DNS server.
Domain name	Domain name suffix.
SIP server addresses	IPv6 address of the SIP server.
SIP server domain names	Domain name of the SIP server.
Options	Self-defined options.
Code	Code of the self-defined option.
Length	Self-defined option length in bytes.
Hex	Self-defined option content represented by a hexadecimal number.

Related commands

ipv6 address dhcp-alloc

ipv6 dhcp client duid

ipv6 dhcp client pd

display ipv6 dhcp client statistics

Use **display ipv6 dhcp client statistics** to display DHCPv6 client statistics.

Syntax

display ipv6 dhcp client statistics [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays statistics for all DHCPv6 clients.

Examples

Display DHCPv6 client statistics on VLAN-interface 2.

```
<Sysname> display ipv6 dhcp client statistics interface vlan-interface 2
Interface                   :  Vlan-interface2
Packets received            :  1
        Reply               :  1
        Advertise           :  0
        Reconfigure         :  0
        Invalid             :  0
Packets sent                :  5
```

```
Solicit             :  0
Request             :  0
Renew               :  0
Rebind              :  0
Information-request :  5
Release             :  0
Decline             :  0
```

Table 14 Command output

Field	Description
Interface	Interface that acts as the DHCPv6 client.
Packets Received	Number of received packets.
Reply	Number of received reply packets.
Advertise	Number of received advertise packets.
Reconfigure	Number of received reconfigure packets.
Invalid	Number of invalid packets.
Packets sent	Number of sent packets.
Solicit	Number of sent solicit packets.
Request	Number of sent request packets.
Renew	Number of sent renew packets.
Rebind	Number of sent rebind packets.
Information-request	Number of sent information request packets.
Release	Number of sent release packets.
Decline	Number of sent decline packets.

Related commands

reset ipv6 dhcp client statistics

ipv6 address dhcp-alloc

Use **ipv6 address dhcp-alloc** to configure an interface to use DHCPv6 for IPv6 address acquisition.

Use **undo ipv6 address dhcp-alloc** to cancel an interface from using DHCPv6, and clear the obtained IPv6 address and other configuration parameters.

Syntax

ipv6 address dhcp-alloc [**option-group** *option-group-number* | **rapid-commit**] *

undo ipv6 address dhcp-alloc

Default

- In a version earlier than R6348P01, an interface does not use DHCPv6 to obtain IPv6 addresses and other network settings.
- In R6348P01 or later, the default setting of this command varies by device startup method as follows:

- When the device starts up with the initial configuration, an interface uses the default settings of software features and does not use DHCPv6 to obtain IPv6 addresses and other network settings.
- When the device starts up with the factory defaults, only VLAN-interface 1 supports using DHCPv6 to obtain IPv6 addresses and other network settings. Other interfaces do not use DHCPv6 to obtain IPv6 addresses and other network settings.

For more information about initial configuration and factory defaults, see configuration file management in *Fundamentals Configuration Guide*.

Views

VLAN interface view

Predefined user roles

network-admin

Parameters

option-group *option-group-number*: Enables the DHCPv6 client to create a dynamic DHCPv6 option group for saving the configuration parameters, and assigns an ID to the option group. The value range for the ID is 1 to 100. If you do not specify this option, the DHCPv6 client does not create any dynamic DHCPv6 option groups.

rapid-commit: Supports rapid address or prefix assignment.

Examples

Configure VLAN-interface 10 to use DHCPv6 for IPv6 address acquisition. Configure the DHCPv6 client to support rapid address assignment and create dynamic DHCPv6 option group 1 for the configuration parameters obtained.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ipv6 address dhcp-alloc rapid-commit option-group 1
```

Related commands

display ipv6 dhcp client

ipv6 dhcp client dscp

Use **ipv6 dhcp client dscp** to set the DSCP value for DHCPv6 packets sent by the DHCPv6 client.

Use **undo ipv6 dhcp client dscp** to restore the default.

Syntax

ipv6 dhcp client dscp *dscp-value*

undo ipv6 dhcp client dscp

Default

The DSCP value in DHCPv6 packets is 56.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Sets the DSCP value for DHCP packets, in the range of 0 to 63.

Usage guidelines

The DSCP value is carried in the Traffic class field of a DHCPv6 packet. It specifies the priority level of the packet and affects the transmission priority of the packet. A bigger DSCP value represents a higher priority.

Examples

Set the DSCP value to 30 for DHCPv6 packets sent by the DHCPv6 client.

```
<Sysname> system-view
[Sysname] ipv6 dhcp client dscp 30
```

ipv6 dhcp client duid

Use **ipv6 dhcp client duid** to configure the DHCPv6 client DUID for an interface.

Use **undo ipv6 dhcp client duid** to restore the default.

Syntax

ipv6 dhcp client duid { **ascii** *ascii-string* | **hex** *hex-string* | **mac** *interface-type interface-number* }

undo ipv6 dhcp client duid

Default

The interface uses the device bridge MAC address to generate its DHCPv6 client DUID.

Views

VLAN interface view

Predefined user roles

network-admin

Parameters

ascii *ascii-string*: Specifies a case-sensitive ASCII string of 1 to 130 characters as the DHCPv6 client DUID.

hex *hex-string*: Specifies a hexadecimal number of 2 to 260 characters as the DHCPv6 client DUID.

mac *interface-type interface-number*: Specifies the MAC address of the specified interface as the DHCPv6 client DUID. The *interface-type interface-number* arguments specify an interface by its type and number.

Usage guidelines

A DHCPv6 client pads its DUID into the Option 1 of the DHCPv6 packet that it sends to the DHCPv6 server. The DHCPv6 server can assign specific IPv6 addresses or prefixes to DHCPv6 clients with specific DUIDs.

The DUID of a DHCPv6 client is the globally unique identifier of the client, so make sure the DUID that you configure is unique.

Examples

Specify the hexadecimal number FFFFFFFF as the DHCPv6 client DUID for VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ipv6 dhcp client duid hex ffffffff
```

Related commands

display ipv6 dhcp client

ipv6 dhcp client pd

Use **ipv6 dhcp client pd** to configure an interface to use DHCPv6 for IPv6 prefix acquisition.

Use **undo ipv6 dhcp client pd** to cancel an interface from using DHCPv6, and clear the obtained IPv6 prefix and other configuration parameters.

Syntax

ipv6 dhcp client pd *prefix-number* [**option-group** *option-group-number* | **rapid-commit**]*

undo ipv6 dhcp client pd

Default

An interface does not use DHCPv6 for IPv6 prefix acquisition.

Views

VLAN interface view

Predefined user roles

network-admin

Parameters

prefix-number: Specifies an IPv6 prefix ID in the range of 1 to 1024. After obtaining an IPv6 prefix, the client assigns the ID to the IPv6 prefix.

rapid-commit: Supports rapid address or prefix assignment.

option-group *option-group-number*: Enables the DHCPv6 client to create a dynamic DHCPv6 option group for saving the configuration parameters, and assigns an ID to the option group. The value range for the ID is 1 to 100. If you do not specify this option, the DHCPv6 client does not create any dynamic DHCPv6 option groups.

Examples

Configure VLAN-interface10 to use DHCPv6 for IPv6 prefix acquisition. Specify IDs for the dynamic IPv6 prefix and dynamic DHCPv6 option group, and configure the client to support rapid prefix assignment.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ipv6 dhcp client pd 1 rapid-commit option-group 1
```

Related commands

display ipv6 dhcp client

ipv6 dhcp client stateful

Use **ipv6 dhcp client stateful** to configure an interface to use DHCPv6 for IPv6 address and prefix acquisition.

Use **undo ipv6 dhcp client stateful** to cancel an interface from using DHCPv6, and clear the obtained IPv6 address, prefix, and other configuration parameters.

Syntax

ipv6 dhcp client stateful prefix *prefix-number* [**option-group** *option-group-number* | **rapid-commit**] *

undo ipv6 dhcp client stateful

Default

An interface does not use DHCPv6 for IPv6 address and prefix acquisition.

Views

VLAN interface view

Predefined user roles

network-admin

Parameters

prefix *prefix-number*: Specifies an IPv6 prefix ID in the range of 1 to 1024. After obtaining an IPv6 prefix, the client assigns the ID to the IPv6 prefix.

rapid-commit: Supports rapid address and prefix assignment.

option-group *option-group-number*: Enables the DHCPv6 client to create a dynamic DHCPv6 option group for saving the configuration parameters, and assigns an ID to the option group. The value range for the ID is 1 to 100. If you do not specify this option, the DHCPv6 client does not create any dynamic DHCPv6 option groups.

Usage guidelines

The **ipv6 dhcp client stateful** command takes effect if it is configured with the **ipv6 address dhcp-alloc** and **ipv6 dhcp client pd** commands on an interface. You must execute the **undo ipv6 dhcp client stateful** command to have the **ipv6 address dhcp-alloc** and **ipv6 dhcp client pd** commands take effect.

Examples

Configure VLAN-interface 10 to use DHCPv6 for IPv6 address and prefix acquisition. Specify IDs for the dynamic IPv6 prefix and dynamic DHCPv6 option group, and configure the client to support rapid address and prefix assignment.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ipv6 dhcp client stateful prefix 1 rapid-commit option-group
1
```

Related commands

ipv6 address dhcp-alloc

ipv6 dhcp client pd

ipv6 dhcp client stateless enable

Use **ipv6 dhcp client stateless enable** to enable stateless DHCPv6.

Use **undo ipv6 dhcp client stateless enable** to disable stateless DHCPv6.

Syntax

ipv6 dhcp client stateless enable

undo ipv6 dhcp client stateless enable

Default

Stateless DHCPv6 is disabled.

Views

VLAN interface view

Predefined user roles

network-admin

Usage guidelines

Stateless DHCPv6 enables the interface to send an Information-request message to the multicast address of all DHCPv6 servers and DHCPv6 relay agents for configuration parameters.

Examples

Enable stateless DHCPv6 on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ipv6 dhcp client stateless enable
```

reset ipv6 dhcp client statistics

Use **reset ipv6 dhcp client statistics** to clear DHCPv6 client statistics.

Syntax

reset ipv6 dhcp client statistics [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command clears all DHCPv6 client statistics.

Examples

Clear all DHCPv6 client statistics.

```
<Sysname> reset ipv6 dhcp client statistics
```

Related commands

display ipv6 dhcp client statistics

DHCPv6 snooping commands

DHCPv6 snooping works between the DHCPv6 client and the DHCPv6 server or between the DHCPv6 client and DHCPv6 the relay agent. DHCPv6 snooping does not work between the DHCPv6 server and the DHCPv6 relay agent.

display ipv6 dhcp snooping binding

Use **display ipv6 dhcp snooping binding** to display DHCPv6 snooping address entries.

Syntax

display ipv6 dhcp snooping binding [**address** *ipv6-address* [**vlan** *vlan-id*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

address *ipv6-address*: Displays the DHCPv6 snooping entry for the specified IPv6 address.

vlan *vlan-id*: Specifies the ID of the VLAN where the IPv6 address resides.

Usage guidelines

If you do not specify any parameters, this command displays all DHCPv6 snooping address entries.

Examples

Display all DHCPv6 snooping address entries.

```
<Sysname> display ipv6 dhcp snooping binding
1 DHCPv6 snooping entries found.
 IPv6 address     MAC address    Lease       VLAN SVLAN Interface
 ================ ============== =========== ==== ===== ========================
 2::1             00e0-fc00-0006 54          2    N/A   GigabitEthernet1/0/1
```

Table 15 Command output

Field	Description
IPv6 Address	IPv6 address assigned to the DHCPv6 client.
MAC Address	MAC address of the DHCPv6 client.
Lease	Remaining lease duration in seconds.
VLAN	When both DHCPv6 snooping and QinQ are enabled or the DHCPv6 packet contains two VLAN tags, this field identifies the outer VLAN tag. Otherwise, it identifies the VLAN where the port connecting the DHCPv6 client resides.
SVLAN	When both DHCPv6 snooping and QinQ are enabled or the DHCPv6 packet contains two VLAN tags, this field identifies the inner VLAN tag. Otherwise, it displays **N/A**.
Interface	Port connecting to the DHCPv6 client.

Related commands

ipv6 dhcp snooping binding record

reset ipv6 dhcp snooping binding

display ipv6 dhcp snooping binding database

Use **display ipv6 dhcp snooping binding database** to display information about DHCPv6 snooping entry auto backup.

Syntax

display ipv6 dhcp snooping binding database

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display information about DHCPv6 snooping entry auto backup.

```
<Sysname> display ipv6 dhcp snooping binding database
File name              :   database.dhcp
Username               :
Password               :
Update interval        :   600 seconds
Latest write time      :   Feb 27 18:48:04 2012
Status                 :   Last write succeeded.
```

Table 16 Command output

Field	Description
File name	Name of the DHCPv6 snooping entry backup file.
Username	Username for accessing the URL of the remote backup file.
Password	Password for accessing the URL of the remote backup file. This field displays ********** if a password is configured.
Update interval	Waiting time in seconds after a DHCPv6 snooping entry change for the DHCPv6 snooping device to update the backup file.
Latest write time	Time of the latest update.
Status	Status of the update: • **Writing**—The backup file is being updated. • **Last write succeeded**—The backup file was successfully updated. • **Last write failed**—The backup file failed to be updated.

display ipv6 dhcp snooping packet statistics

Use **display ipv6 dhcp snooping packet statistics** to display DHCPv6 packet statistics for DHCPv6 snooping.

Syntax

display ipv6 dhcp snooping packet statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays DHCPv6 packet statistics for the master device.

Examples

Display DHCPv6 packet statistics for DHCPv6 snooping.

```
<Sysname> display ipv6 dhcp snooping packet statistics
 DHCPv6 packets received                 : 100
 DHCPv6 packets sent                     : 200
 Invalid DHCPv6 packets dropped          : 0
```

Related commands

reset ipv6 dhcp snooping packet statistics

display ipv6 dhcp snooping pd binding

Use **display ipv6 dhcp snooping pd binding** to display DHCPv6 snooping prefix entries.

Syntax

display ipv6 dhcp snooping pd binding [**prefix** *prefix/prefix-length* [**vlan** *vlan-id*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

prefix *prefix/prefix-length*: Specifies an IPv6 prefix with its length. The value range for the *prefix-length* argument is 1 to 128.

vlan *vlan-id*: Specifies the ID of the VLAN where the IPv6 prefix resides. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

This command takes effect only after you execute the **ipv6 dhcp snooping pd binding record** command on the port directly connecting to the clients.

If you do not specify any parameters, this command displays all DHCPv6 snooping prefix entries.

Examples

Display all DHCPv6 snooping prefix entries.

```
<Sysname> display ipv6 dhcp snooping pd binding
1 DHCPv6 snooping PD entries found.
IPv6 prefix      Lease       VLAN SVLAN Interface
================ =========== ==== ===== ========================
1:2::/64         54          2    N/A   GigabitEthernet1/0/1
```

Table 17 Command output

Field	Description
n DHCPv6 snooping PD entries found.	Total number of DHCPv6 snooping prefix entries.
IPv6 prefix	IPv6 prefix assigned to the DHCPv6 client.
Lease	Remaining lease duration in seconds.

Field	Description
VLAN	When both DHCPv6 snooping and QinQ are enabled or the DHCPv6 packet contains two VLAN tags, this field identifies the outer VLAN tag. Otherwise, it identifies the VLAN where the port connecting the DHCPv6 client resides.
SVLAN	When both DHCPv6 snooping and QinQ are enabled or the DHCPv6 packet contains two VLAN tags, this field identifies the inner VLAN tag. Otherwise, it displays **N/A**.
Interface	Port connecting to the DHCPv6 client.

Related commands

`ipv6 dhcp snooping pd binding record`

`reset ipv6 dhcp snooping pd binding`

display ipv6 dhcp snooping trust

Use **`display ipv6 dhcp snooping trust`** to display information about trusted ports.

Syntax

`display ipv6 dhcp snooping trust`

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display information about trusted ports.

```
<Sysname> display ipv6 dhcp snooping trust
DHCPv6 snooping is enabled.
Interface                           Trusted             VLAN
============================        ============        =======
GE1/0/1                             -                   100
GE1/0/2                             Trusted             -

VSI name                            Tunnel trusted
============================        ============
a                                   Trusted

AC                                  Trusted
============================        ============
```

Table 18 Command output

Field	Description
Interface	Interface name.

Field	Description
Trusted	Trusted port specified in global DHCPv6 snooping configuration. If the trusted port is specified in VLAN-based DHCPv6 snooping configuration, this field displays a hyphen (**-**).
VLAN	VLAN to which the trusted port belongs. If the trusted port is specified in global DHCPv6 snooping configuration, this field displays a hyphen (**-**).
VSI name	This field is not supported in the current software version. VSI name of the VXLAN tunnel interface. This field is available when you configure the tunnel interface assigned to the VSI as a DHCP snooping trusted interface by using the **ipv6 dhcp snooping trust tunnel** command.
Tunnel trusted	This field is not supported in the current software version. Trusted tunnel interface specified in VXLAN-based DHCPv6 snooping configuration.
AC	This field is not supported in the current software version. AC name, which is indicated by the interface name and Ethernet service instance name. This field is available when you configure the AC as the DHCPv6 snooping trusted interface by using the **ipv6 dhcp snooping trust** command in Ethernet service instance view.
Trusted	This field is not supported in the current software version. Trusted AC specified in VXLAN-based DHCPv6 snooping configuration.

Related commands

ipv6 dhcp snooping trust

ipv6 dhcp snooping binding database filename

Use **ipv6 dhcp snooping binding database filename** to configure the DHCPv6 snooping device to back up DHCPv6 snooping entries to a file.

Use **undo ipv6 dhcp snooping binding database filename** to disable the auto backup and remove the backup file.

Syntax

ipv6 dhcp snooping binding database filename { *filename* | **url** *url* [**username** *username* [**password** { **cipher** | **simple** } *string*]] }

undo ipv6 dhcp snooping binding database filename

Default

The DHCPv6 snooping device does not back up DHCPv6 snooping entries.

Views

System view

Predefined user roles

network-admin

Parameters

filename: Specifies the name of a local backup file. For information about the *filename* argument, see *Fundamentals Configuration Guide*.

url *url*: Specifies the URL of a remote backup file. The URL is a case-sensitive string of 1 to 255 characters. Do not include a username or password in the URL. The supported path format type varies by server.

username *username*: Specifies the username for accessing the URL of the remote backup file. The username is a case-sensitive string of 1 to 32 characters. Do not specify this option if a username is not required for accessing the URL.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 32 characters. Its encrypted form is a case-sensitive string of 1 to 73 characters. Do not specify this argument if a password is not required for accessing the URL of the remote backup file.

Usage guidelines

This command automatically creates the file if you specify a nonexistent file.

With this command executed, the DHCPv6 snooping device backs up its snooping entries immediately and runs auto backup. The snooping device, by default, waits 300 seconds after a DHCPv6 snooping entry change to update the backup file. You can use the **ipv6 dhcp snooping binding database update interval** command to change the waiting time. If no DHCPv6 snooping entry changes, the backup file is not updated.

As a best practice, back up the DHCPv6 snooping entries to a remote file. If you use the local storage medium, the frequent erasing and writing might damage the medium and then cause the DHCPv6 snooping device malfunction.

When the file is on a remote device, follow these restrictions and guidelines to specify the URL, username, and password:

- If the file is on an FTP server, enter URL in the format of ftp:*//server address:port/file path*, where the port number is optional.
- If the file is on a TFTP server, enter URL in the format of tftp:*//server address:port/file path*, where the port number is optional.
- The username and password must be the same as those configured on the FTP server. If the server authenticates only the username, the password can be omitted.
- If the IP address of the server is an IPv6 address, enclose the address in a pair of brackets, for example, **ftp://[1::1]/database.dhcp**.
- You can also specify the DNS domain name for the server address field, for example, **ftp://company/database.dhcp**.

Examples

Configure the DHCPv6 snooping device to back up DHCPv6 snooping entries to the file **database.dhcp**.

```
<Sysname> system-view
[Sysname] ipv6 dhcp snooping binding database filename database.dhcp
```

Configure the DHCPv6 snooping device to back up DHCPv6 snooping entries to the file **database.dhcp** in the working directory of the FTP server at 1::1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp snooping binding database filename url ftp://[1::1]/database.dhcp
username 1 password simple 1
```

Configure the DHCPv6 snooping device to back up DHCPv6 snooping entries to the file **database.dhcp** in the working directory of the TFTP server at 2::1.

```
<Sysname> system-view
[Sysname] ipv6 dhcp snooping binding database filename url tftp://[2::1]/database.dhcp
```

Related commands

ipv6 dhcp snooping binding database update interval

ipv6 dhcp snooping binding database update interval

Use **ipv6 dhcp snooping binding database update interval** to set the waiting time for the DHCPv6 snooping device to update the backup file after a DHCPv6 snooping entry change.

Use **undo ipv6 dhcp snooping binding database update interval** to restore the default.

Syntax

ipv6 dhcp snooping binding database update interval *interval*

undo ipv6 dhcp snooping binding database update interval

Default

The DHCPv6 snooping device waits 300 seconds to update the backup file after a DHCPv6 snooping entry change. If no DHCPv6 snooping entry changes, the backup file is not updated.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Sets the waiting time in seconds, in the range of 60 to 864000.

Usage guidelines

When a DHCPv6 snooping entry is learned, updated, or removed, the waiting period starts. The DHCPv6 snooping device updates the backup file when the waiting period is reached. All snooping entries changed during the period will be saved to the backup file.

The waiting time takes effect only after you configure the DHCPv6 snooping entry auto backup by using the **ipv6 dhcp snooping binding database filename** command.

Examples

Set the waiting time to 600 seconds for the DHCPv6 snooping device to update the backup file.

```
<Sysname> system-view
[Sysname] ipv6 dhcp snooping binding database update interval 600
```

Related commands

ipv6 dhcp snooping binding database filename

ipv6 dhcp snooping binding database update now

Use **ipv6 dhcp snooping binding database update now** to manually save DHCPv6 snooping entries to the backup file.

Syntax

ipv6 dhcp snooping binding database update now

Views

System view

Predefined user roles

network-admin

Usage guidelines

Each time this command is executed, the DHCPv6 snooping entries are saved to the backup file.

This command takes effect only after you configure the DHCPv6 snooping entry auto backup by using the **ipv6 dhcp snooping binding database filename** command.

Examples

Manually save DHCPv6 snooping entries to the backup file.

```
<Sysname> system-view
[Sysname] ipv6 dhcp snooping binding database update now
```

Related commands

ipv6 dhcp snooping binding database filename

ipv6 dhcp snooping binding record

Use **ipv6 dhcp snooping binding record** to enable recording DHCPv6 snooping address entries.

Use **undo ipv6 dhcp snooping binding record** to disable recording DHCPv6 snooping address entries.

Syntax

ipv6 dhcp snooping binding record

undo ipv6 dhcp snooping binding record

Default

Recording of DHCPv6 snooping address entries is disabled.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

VLAN view

Predefined user roles

network-admin

Usage guidelines

You can configure this command on the ports that are directly connected to the DHCPv6 clients.

This command enables DHCPv6 snooping to record IP-to-MAC information of the DHCPv6 clients (called DHCPv6 snooping address entries).

Examples

Enable recording DHCPv6 snooping address entries on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping binding record
```

ipv6 dhcp snooping check request-message

Use **ipv6 dhcp snooping check request-message** to enable the DHCPv6-REQUEST check feature.

Use **undo ipv6 dhcp snooping check request-message** to disable the DHCPv6-REQUEST check feature.

Syntax

ipv6 dhcp snooping check request-message

undo ipv6 dhcp snooping check request-message

Default

The DHCPv6-REQUEST check feature is disabled.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

Use the DHCPv6-REQUEST check feature to protect the DHCPv6 server against DHCPv6 client spoofing attacks. The feature enables the DHCPv6 snooping device to check every received DHCPv6-RENEW, DHCPv6-DECLINE, or DHCPv6-RELEASE message against DHCPv6 snooping entries.

- If any criterion in an entry is matched, the device compares the entry with the message information.
  - If they are consistent, the device considers the message valid and forwards it to the DHCPv6 server.
  - If they are different, the device considers the message forged and discards it.
- If no matching entry is found, the device forwards the message to the DHCPv6 server.

Examples

Enable DHCPv6-REQUEST check.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping check request-message
```

ipv6 dhcp snooping deny

Use **ipv6 dhcp snooping deny** to configure a port as DHCPv6 packet blocking port.

Use **undo ipv6 dhcp snooping deny** to restore the default.

Syntax

ipv6 dhcp snooping deny

undo ipv6 dhcp snooping deny

Default

A port does not block DHCPv6 requests.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

CAUTION:

To avoid IPv6 address and prefix acquisition failure, configure a port to block DHCPv6 packets only if no DHCPv6 clients are connected to it.

To enable a port on the snooping device to drop all incoming DHCPv6 requests, configure that port as a DHCPv6 packet blocking port.

Examples

Configure GigabitEthernet 1/0/1 as a DHCPv6 packet blocking port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping deny
```

ipv6 dhcp snooping disable

Use **ipv6 dhcp snooping disable** to disable DHCP snooping.

Use **undo ipv6 dhcp snooping disable** to restore the default.

Syntax

ipv6 dhcp snooping disable

undo ipv6 dhcp snooping disable

Default

If you enable DHCPv6 snooping globally or for a VLAN, DHCP snooping is enabled on all interfaces on the device or on all interfaces in the VLAN.

If you do not enable DHCPv6 snooping globally or for a VLAN, DHCP snooping is disabled on all interfaces on the device or on all interfaces in the VLAN.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

This command allows you to narrow down the interface range where DHCPv6 snooping takes effect. For example, to enable DHCPv6 snooping globally except for a specific interface, you can enable DHCPv6 snooping globally and execute this command on the target interface.

Examples

Disable DHCPv6 snooping on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping disable
```

Related commands

ipv6 dhcp snooping enable

ipv6 dhcp snooping enable vlan

ipv6 dhcp snooping enable

Use **ipv6 dhcp snooping enable** to enable DHCPv6 snooping.

Use **undo ipv6 dhcp snooping enable** to disable DHCPv6 snooping.

Syntax

ipv6 dhcp snooping enable

undo ipv6 dhcp snooping enable

Default

DHCPv6 snooping is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Use the DHCPv6 snooping feature together with trusted port configuration. Trusted ports forward responses from DHCPv6 servers and untrusted ports discard responses from DHCPv6 servers. This mechanism ensures that DHCPv6 clients obtain IPv6 addresses or prefixes from authorized DHCPv6 servers.

When DHCPv6 snooping is disabled, all ports on the device forward responses from DHCPv6 servers.

Examples

Enable DHCPv6 snooping.

```
<Sysname> system-view
[Sysname] ipv6 dhcp snooping enable
```

Related commands

ipv6 dhcp snooping disable

ipv6 dhcp snooping enable vlan

Use **ipv6 dhcp snooping enable vlan** to enable DHCPv6 snooping for VLANs.

Use **undo ipv6 dhcp snooping enable vlan** to disable DHCPv6 snooping for VLANs.

Syntax

ipv6 dhcp snooping enable vlan *vlan-id-list*

undo ipv6 dhcp snooping enable vlan *vlan-id-list*

Default

DHCPv6 snooping is disabled for all VLANs.

Views

System view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 VLAN items. Each VLAN item specifies a VLAN by VLAN ID or specifies a range of VLANs in the form of *vlan-id1* to *vlan-id2*. The value range for the VLAN IDs is 1 to 4094. If you specify a VLAN range, the value for the *vlan-id2* argument must be greater than the value for the *vlan-id1* argument.

Usage guidelines

After you enable DHCPv6 snooping for a VLAN, DHCPv6 snooping untrusted ports in the VLAN discard incoming DHCP responses. This mechanism ensures that DHCP clients obtain IP addresses from authorized DHCP servers.

After you disable DHCPv6 snooping for a VLAN, all interfaces in the VLAN can forward DHCPv6 responses.

After you enable DHCPv6 snooping globally, all VLANs on the device are also enabled with DHCPv6 snooping. To disable DHCPv6 snooping in a VLAN, disable DHCPv6 snooping globally and in the VLAN.

Examples

Enable DHCPv6 snooping for VLANs 5,10, 20, and 32.

```
<Sysname> system-view
[Sysname] ipv6 dhcp snooping enable vlan 5 10 to 20 32
```

Related commands

ipv6 dhcp snooping disable

ipv6 dhcp snooping trust interface

ipv6 dhcp snooping log enable

Use **ipv6 dhcp snooping log enable** to enable DHCPv6 snooping logging.

Use **undo ipv6 dhcp snooping log enable** to disable DHCPv6 snooping logging.

Syntax

ipv6 dhcp snooping log enable

undo ipv6 dhcp snooping log enable

Default

DHCPv6 snooping logging is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command enables the DHCPv6 snooping device to generate DHCPv6 snooping logs and send them to the information center. The log information helps administrators locate and solve problems. For information about the log destination and output rule configuration in the information center, see *Network Management and Monitoring Configuration Guide*.

As a best practice, disable this feature if the log generation affects the device performance.

Examples

Enable DHCPv6 snooping logging.

```
<Sysname> system-view
[Sysname] ipv6 dhcp snooping log enable
```

ipv6 dhcp snooping option interface-id enable

Use **ipv6 dhcp snooping option interface-id enable** to enable support for the interface-ID option (also called Option 18).

Use **undo ipv6 dhcp snooping option interface-id enable** to disable support for the interface-ID option.

Syntax

ipv6 dhcp snooping option interface-id enable

undo ipv6 dhcp snooping option interface-id enable

Default

Option 18 is not supported.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only when DHCPv6 snooping is globally enabled.

Examples

Enable support for Option 18.

```
<Sysname> system-view
[Sysname] ipv6 dhcp snooping enable
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping option interface-id enable
```

Related commands

ipv6 dhcp snooping enable

ipv6 dhcp snooping option interface-id string

ipv6 dhcp snooping option interface-id string

Use **ipv6 dhcp snooping option interface-id string** to specify the content as the interface ID for Option 18.

Use **undo ipv6 dhcp snooping option interface-id string** to restore the default.

Syntax

ipv6 dhcp snooping option interface-id [**vlan** *vlan-id*] **string** *interface-id*

undo ipv6 dhcp snooping option interface-id [**vlan** *vlan-id*] **string**

Default

The DHCPv6 snooping device uses its DUID as the content for Option 18.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan *vlan-id*: Pads the interface ID for packets received from the specified VLAN. If you do not specify a VLAN, the device pads the interface ID for packets received from the default VLAN.

interface-id: Specifies a string of 1 to 128 characters as the interface ID.

Examples

Specify **company001** as the interface ID.

```
<Sysname> system-view
[Sysname] ipv6 dhcp snooping enable
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping option interface-id enable
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping option interface-id string company001
```

Related commands

ipv6 dhcp snooping enable

ipv6 dhcp snooping option interface-id enable

ipv6 dhcp snooping option remote-id enable

Use **ipv6 dhcp snooping option remote-id enable** to enable support for the remote-ID option (also called Option 37).

Use **undo ipv6 dhcp snooping option remote-id enable** to disable support for the remote-ID option.

Syntax

ipv6 dhcp snooping option remote-id enable

undo ipv6 dhcp snooping option remote-id enable

Default

Option 37 is not supported.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only when DHCPv6 snooping is globally enabled.

Examples

Enable support for Option 37.

```
<Sysname> system-view
[Sysname] ipv6 dhcp snooping enable
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping option remote-id enable
```

Related commands

ipv6 dhcp snooping enable

ipv6 dhcp snooping option remote-id string

ipv6 dhcp snooping option remote-id string

Use **ipv6 dhcp snooping option remote-id string** to specify the content as the remote ID for Option 37.

Use **undo ipv6 dhcp snooping option remote-id string** to restore the default.

Syntax

ipv6 dhcp snooping option remote-id [**vlan** *vlan-id*] **string** *remote-id*

undo ipv6 dhcp snooping option remote-id [**vlan** *vlan-id*] **string**

Default

The DHCPv6 snooping device uses its DUID as the content for Option 37.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan *vlan-id*: Pads the remote ID for packets received from the specified VLAN. If you do not specify a VLAN, the device pads the remote ID for packets received from the default VLAN.

remote-id: Specifies a string of 1 to 128 characters as the remote ID.

Examples

Specify **device001** as the remote ID.

```
<Sysname> system-view
[Sysname] ipv6 dhcp snooping enable
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping option remote-id enable
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping option remote-id string device001
```

Related commands

ipv6 dhcp snooping enable

ipv6 dhcp snooping option remote-id enable

ipv6 dhcp snooping pd binding record

Use **ipv6 dhcp snooping pd binding record** to enable recording DHCPv6 snooping prefix entries.

Use **undo ipv6 dhcp snooping pd binding record** to disable recording DHCPv6 snooping prefix entries.

Syntax

ipv6 dhcp snooping pd binding record

undo ipv6 dhcp snooping pd binding record

Default

Recording of DHCPv6 snooping prefix entries is disabled.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

VLAN view

Predefined user roles

network-admin

Usage guidelines

This command enables DHCPv6 snooping to record IPv6 prefix-to-port information of the DHCPv6 clients (called DHCPv6 snooping prefix entries). When IP source guard (IPSG) is configured on the DHCP snooping device, IPSG can generate dynamic bindings based on the DHCP snooping prefix entries to filter out illegitimate packets.

Examples

Enable DHCPv6 snooping prefix entries on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname]interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping pd binding record
```

Related commands

display ipv6 dhcp snooping pd binding

ipv6 dhcp snooping rate-limit

Use **ipv6 dhcp snooping rate-limit** to enable DHCPv6 snooping packet rate limit on an interface and set the limit value.

Use **undo ipv6 dhcp snooping rate-limit** to disable DHCPv6 snooping packet rate limit.

Syntax

ipv6 dhcp snooping rate-limit *rate*

undo ipv6 dhcp snooping rate-limit

Default

The DHCPv6 snooping packet rate limit is disabled on an interface.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

rate: Specifies the maximum rate in Kbps. The value range is 64 to 512.

Usage guidelines

This command takes effect only when DHCPv6 snooping is enabled.

The DHCPv6 packet rate limit feature enables the interface to discard DHCPv6 packets that exceed the maximum rate.

The rate configured on a Layer 2 aggregate interface applies to all members of the aggregate interface. If a member interface leaves the aggregation group, it uses the rate configured in its Ethernet interface view.

The chip-supported maximum rate is an integer multiple of eight. If you set the maximum rate to 67, the value 64 or 72 takes effect.

Examples

Configure GigabitEthernet 1/0/1 to receive DHCPv6 packets at a maximum rate of 64 Kbps.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping rate-limit 64
```

ipv6 dhcp snooping trust

Use **ipv6 dhcp snooping trust** to configure a port as a trusted port.

Use **undo ipv6 dhcp snooping trust** to restore the default state of a port.

Syntax

ipv6 dhcp snooping trust

undo ipv6 dhcp snooping trust

Default

After you enable DHCPv6 snooping, all ports are untrusted.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

Specify the port facing the DHCP server as trusted and specify the other ports as untrusted so DHCP clients can obtain valid IP addresses.

Examples

Specify GigabitEthernet 1/0/1 as a trusted port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping trust
```

Related commands

display ipv6 dhcp snooping trust

ipv6 dhcp snooping trust interface

Use **ipv6 dhcp snooping trust interface** to configure a port in a VLAN as a DHCPv6 snooping trusted port.

Use **undo ipv6 dhcp snooping trust interface** to restore the default state of a port in a VLAN.

Syntax

ipv6 dhcp snooping trust interface *interface-type interface-number*

undo ipv6 dhcp snooping trust interface *interface-type interface-number*

Default

After you enable DHCPv6 snooping for a VLAN, all ports in the VLAN are DHCP snooping untrusted ports.

Views

VLAN view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

In a VLAN, specify the port facing the DHCP server as trusted and specify the other ports as untrusted so DHCP clients can obtain valid IP addresses.

You can execute this command multiple times in a VLAN to configure multiple trusted ports in the VLAN.

Make sure the specified port is in the VLAN for which the **ipv6 dhcp snooping enable vlan** command is configured.

Examples

In VLAN 1, configure GigabitEthernet 1/0/1 as a trusted port.

```
<Sysname> system-view
[Sysname] vlan 1
[Sysname-vlan1] ipv6 dhcp snooping trust interface gigabitethernet 1/0/1
```

Related commands

ipv6 dhcp snooping enable vlan

reset ipv6 dhcp snooping binding

Use **reset ipv6 dhcp snooping binding** to clear DHCPv6 snooping address entries.

Syntax

reset ipv6 dhcp snooping binding { **all** | **address** *ipv6-address* [**vlan** *vlan-id*] }

Views

User view

Predefined user roles

network-admin

Parameters

address *ipv6-address*: Clears the DHCPv6 snooping entry for the specified IPv6 address.

vlan *vlan-id*: Clears DHCPv6 snooping address entries for the specified VLAN. If you do not specify a VLAN, this command clears DHCPv6 snooping address entries for the default VLAN.

all: Clears all DHCPv6 snooping address entries.

Examples

Clear all DHCPv6 snooping address entries.

```
<Sysname> reset ipv6 dhcp snooping binding all
```

Related commands

display ipv6 dhcp snooping binding

reset ipv6 dhcp snooping packet statistics

Use **reset ipv6 dhcp snooping packet statistics** to clear DHCPv6 packet statistics for DHCPv6 snooping.

Syntax

reset ipv6 dhcp snooping packet statistics [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears DHCPv6 packet statistics for the master device.

Examples

Clear DHCPv6 packet statistics for DHCPv6 snooping.

```
<Sysname> reset ipv6 dhcp snooping packet statistics
```

Related commands

display ipv6 dhcp snooping packet statistics

reset ipv6 dhcp snooping pd binding

Use **reset ipv6 dhcp snooping pd binding** to clear DHCPv6 snooping prefix entries.

Syntax

reset ipv6 dhcp snooping pd binding { **all** | **prefix** *prefix/prefix-length* [**vlan** *vlan-id*] }

Views

User view

Predefined user roles

network-admin

Parameters

all: Clears all DHCPv6 snooping prefix entries.

prefix *prefix/prefix-length*: Clears DHCPv6 snooping entries for the specified IPv6 prefix. The value range for the *prefix-length* argument is 1 to 128.

vlan *vlan-id*: Clears DHCPv6 snooping prefix entries for the specified VLAN. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

If you do not specify any parameters, this command clears all DHCPv6 snooping prefix entries.

Examples

Clear DHCPv6 snooping prefix entries for 1:2::/64.

```
<Sysname> reset ipv6 dhcp snooping pd binding prefix 1:2::/64
```

Related commands

display ipv6 dhcp snooping pd binding

DHCPv6 guard commands

The DHCPv6 guard feature operates correctly only when the device is located between the DHCPv6 client and the DHCPv6 server or between the DHCPv6 client and the DHCPv6 relay agent. If the device is located between the DHCPv6 server and the DHCPv6 relay agent, the DHCPv6 guard feature cannot operate correctly.

When the DHCPv6 guard feature is configured on a DHCPv6 snooping device, both features can take effect. The device forwards DHCPv6 reply packets received on a DHCP snooping trusted port only if they pass the DHCPv6 guard check. These packets are dropped if they fail the DHCPv6 guard check.

device-role

Use **device-role** to set the role of the device attached to the target interface or VLAN.

Use **undo device-role** to restore the default.

Syntax

device-role { **client** | **server** }

undo device-role

Default

The role is DHCPv6 client for the device attached to the target interface or VLAN.

Views

DHCPv6 guard policy view

Predefined user roles

network-admin

Parameters

client: Sets the device role to DHCPv6 client.

server: Sets the device role to DHCPv6 server.

Usage guidelines

The target interface or VLAN refers to the interface or VLAN to which a DHCPv6 guard policy is applied. The device makes forwarding decisions based on the device role as follows:

- Drops DHCPv6 replies received from the device with the device role of DHCPv6 client.
- Forwards DHCP replies received from the device with the device role of DHCPv6 server only if the packets pass the DHCPv6 guard check.

If the target interface or VLAN is attached to an authorized DHCPv6 server, set the device role to DHCPv6 server for the authorized DHCPv6 server. If no authorized DHCP servers are attached to the target interface or VLAN, set the device role to DHCPv6 client for devices attached to the target interface or VLAN.

The **trust port** command has a higher priority than the **device-role** command. If you configure both commands for a DHCPv6 guard policy, the **trust port** command takes effect.

Examples

Set the role to DHCPv6 server for the device attached to the target interface or VLAN.

```
<Sysname> system-view
[Sysname] ipv6 dhcp guard policy p1
[Sysname-dhcp6-guard-policy-p1] device-role server
```

display ipv6 dhcp guard policy

Use **display ipv6 dhcp guard policy** to display information about DHCPv6 guard policies.

Syntax

display ipv6 dhcp guard policy [*policy-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

policy-name: Displays detailed information about a DHCPv6 guard policy. This argument specifies the name of a DHCPv6 guard policy, a case-insensitive string of 1 to 63 characters. If you do not specify this argument, the command displays brief information about all DHCPv6 guard policies.

Examples

Display detailed information about DHCPv6 guard policy **p1**.

```
<Sysname> display ipv6 dhcp guard policy p1
Guard policy: p1
  Device-role: Server
  Trusted port: No
  Server preference min value: 23
  Server preference max value: 45
  Server rule: ACL sed
  Reply rule: ACL 3434
  Applied to interfaces: GE1/0/1, GE1/0/2
  Applied to VLANs: 100
```

Display brief information about all DHCPv6 guard policies.

```
<Sysname> display ipv6 dhcp guard policy
Guard policy: p1
  Device-role: server
  Trusted port: No
  Server preference min value: 23
  Server preference max value: 45
  Server rule: ACL sed
  Reply rule: ACL 3434
```

```
Guard policy: p2
  Device-role: Server
  Trusted port: Yes
  Server preference min value: 12
  Server preference max value: 34
```

Table 19 Command output

Field	Description
Guard policy	DHCPv6 guard policy name.
Device-role	Device role: • **Client**—DHCPv6 client role. • **Server**—DHCPv6 server role.
Trusted port	Whether the trusted port is configured for the guard policy.
Server preference min value	Minimum preference value of the DHCPv6 server. This field is displayed only when the **preference min** command is configured.
Server preference max value	Maximum preference value of the DHCPv6 server. This field is displayed only when the **preference max** command is configured.
Server rule	DHCP server address match criterion. This field is displayed only when the **if-match server acl** command is configured.
Reply rule	Match criterion for the assigned IPv6 addresses/prefixes. This field is displayed only when the **if-match reply acl** command is configured.
Applied to interfaces	Interfaces to which the DHCPv6 guard policy is applied. Interfaces are separated by commas (,). This field is not displayed when the command displays brief information about DHCPv6 guard policies.
Applied to VLANs	VLANs to which the DHCPv6 guard policy is applied. VLANs are separated by commas (,). This field is not displayed when the command displays brief information about DHCPv6 guard policies.

Related commands

ipv6 dhcp guard policy

if-match reply acl

Use **if-match reply acl** to configure a match criterion for IPv6 addresses/prefixes assigned by a DHCPv6 server.

Use **undo if-match server acl** to restore the default.

Syntax

if-match reply acl { *acl-number* | **name** *acl-name* }

undo if-match reply acl

Default

No match criterion is configured for the assigned IPv6 addresses/prefixes, and all assigned IPv6 addresses/prefixes can pass the address/prefix check.

Views

DHCPv6 guard policy view

Predefined user roles

network-admin

Parameters

acl-number: Specifies an ACL number. The value range for this argument is as follows:

- . 2000 to 2999 for a basic ACL.
- . 3000 to 3999 for an advanced ACL.

name *acl-name*: Specifies a basic or advanced ACL by its name, a case-insensitive string of 1 to 63 characters. The ACL name must start with an English letter and to avoid confusion, it cannot be **all**.

Usage guidelines

The device uses the source IPv6 address attributes in the specified ACL to match the assigned IPv6 address/prefix in the received DHCPv6 Reply message.

- If the assigned IPv6 address/prefix matches a permit statement in the ACL, the device forwards the Reply message. If the assigned IPv6 address/prefix does not match the ACL, the device drops the Reply message.
- If the ACL does not have any source IPv6 address attributes, all DHCPv6 Reply messages fail the address/prefix check and are dropped.
- If the ACL does not exist or does not have any rules, all DHCPv6 Reply messages can pass the check.

If you execute this command multiple times for a DHCPv6 guard policy, the most recent configuration takes effect.

Examples

Specify ACL 2233 to match IPv6 addresses/prefixes assigned by a DHCPv6 server.

```
<Sysname> system-view
[Sysname] ipv6 dhcp guard policy p1
[Sysname-dhcp6-guard-policy-p1] if-match reply acl 2233
```

Related commands

acl (*ACL and QoS Command Reference*)

rule (IPv6 advanced ACL view) (*ACL and QoS Command Reference*)

rule (IPv6 basic ACL view) (*ACL and QoS Command Reference*)

if-match server acl

Use **if-match server acl** to configure a DHCPv6 server match criterion

Use **undo if-match server acl** to restore the default.

Syntax

if-match server acl { *acl-number* | **name** *acl-name* }

undo if-match server acl

Default

No DHCP server match criterion is configured, and all DHCPv6 servers are authorized.

Views

DHCPv6 guard policy view

Predefined user roles

network-admin

Parameters

acl-number: Specifies an ACL number. The value range for this argument is as follows:

- . 2000 to 2999 for a basic ACL.
- . 3000 to 3999 for an advanced ACL.

name *acl-name*: Specifies a basic or advanced ACL by its name, a case-insensitive string of 1 to 63 characters. The ACL name must start with an English letter and to avoid confusion, it cannot be **all**.

Usage guidelines

The device uses the source IPv6 address attributes in the specified ACL to match the source IPv6 address in the received DHCPv6 Advertise message.

- If the source IPv6 address matches a permit statement in the ACL, the device continues to use other criterion to verify the message. If the source IPv6 address does not match the ACL, the device drops the Advertise message.
- If the ACL does not have any source IPv6 address attributes, all DHCPv6 Advertise messages fail the address check and are dropped.
- If the ACL does not exist or does not have any rules, all DHCPv6 Advertise messages can pass the check.

If you execute this command multiple times for a DHCPv6 guard policy, the most recent configuration takes effect.

Examples

Specify ACL 2323 to match DHCPv6 servers.

```
<Sysname> system-view
[Sysname] ipv6 dhcp guard policy p1
[Sysname-dhcp6-guard-policy-p1] if-match server acl 2323
```

Related commands

acl (*ACL and QoS Command Reference*)

rule (IPv6 advanced ACL view) (*ACL and QoS Command Reference*)

rule (IPv6 basic ACL view) (*ACL and QoS Command Reference*)

ipv6 dhcp guard apply policy

Use **ipv6 dhcp guard apply policy** to apply a DHCPv6 guard policy to an interface or a VLAN.

Use **undo ipv6 dhcp guard apply policy** to restore the default.

Syntax

ipv6 dhcp guard apply policy *policy-name*

undo ipv6 dhcp guard apply policy

Default

No DHCPv6 guard policy is applied to an interface or VLAN.

Views

Interface view

VLAN view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a DHCPv6 guard policy name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

The DHCPv6 guard policy applied to an interface checks all incoming DHCP replies if the interface is not configured as a trusted port for the DHCPv6 guard policy.

The DHCPv6 guard policy applied to a VLAN checks all incoming DHCP replies if the interfaces in the VLAN are not configured as trusted ports for the DHCPv6 guard policy.

If you apply a nonexistent DHCPv6 guard policy to an interface or VLAN, the device forwards received DHCPv6 replies without check.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Apply DHCPv6 guard policy **p1** to GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp guard apply policy p1
```

Apply DHCPv6 guard policy **p1** to VLAN 100.

```
<Sysname> system-view
[Sysname] vlan 100
[Sysname-vlan100] ipv6 dhcp guard apply policy p1
```

Related commands

ipv6 dhcp guard policy

ipv6 dhcp guard policy

Use **ipv6 dhcp guard policy** to create a DHCPv6 guard policy and enter its view, or enter the view of an existing DHCPv6 guard policy.

Use **undo ipv6 dhcp guard policy** to delete a DHCPv6 guard policy.

Syntax

ipv6 dhcp guard policy *policy-name*

undo ipv6 dhcp guard policy *policy-name*

Default

No DHCPv6 guard policies exist.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a DHCPv6 guard policy name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

To provide finer level of filtering granularity, you can specify the following parameters for a DHCPv6 guard policy:

- Device role of the device that attached to the target interface or VLAN.
- DHCPv6 server match criterion.
- Match criterion for IPv6 addresses/prefixes assigned by DHCPv6 servers.
- Allowed DHCPv6 server preference range.

The DHCPv6 guard feature runs correctly after you create a DHCPv6 guard policy and apply it to a VLAN or an interface. The DHCPv6 guard feature determines whether to forward DHCP replies based on the match criteria. Only packets that match all criteria are forwarded.

Examples

Create DHCPv6 guard policy **p1** and enter its view.

```
<Sysname> system-view
[Sysname] ipv6 dhcp guard policy p1
[Sysname-dhcp6-guard-policy-p1]
```

Related commands

display ipv6 dhcp guard policy

ipv6 dhcp guard apply policy

preference

Use **preference** to specify an allowed DHCPv6 server preference range.

Use **undo preference** to restore the maximum or minimum preference to the default value.

Syntax

preference { **max** *max-value* | **min** *min-value* } *

undo preference [**max** | **min**]

Default

No DHCPv6 server preference range is configured, and DHCPv6 servers with preferences 1 to 255 can pass the preference check.

Views

DHCPv6 guard policy view

Predefined user roles

network-admin

Parameters

max *max-value*: Specifies the maximum value of the DHCPv6 server preference, in the range of 1 to 255. The default is 255.

min *min-value*: : Specifies the minimum value of the DHCPv6 server preference, in the range of 1 to 255. The default is 1. The minimum value cannot be higher than the maximum value.

Usage guidelines

The device uses the specified range to match the DHCPv6 server preference in the received DHCPv6 Advertise message.

- If the DHCPv6 server preference is in the allowed range, the device continues to use other criterion to further match the message.
- If the DHCPv6 server preference in the Advertise message is beyond the allowed range or the message does not carry the preference, the device drops the message.

When an H3C device acts as a DHCPv6 server, use the **ipv6 dhcp server preference** command to set the preference of the DHCPv6 server.

If you execute this command multiple times for a DHCPv6 guard policy, the most recent configuration takes effect.

Examples

Set the allowed range to 1 to 100 for the DHCPv6 server preference.

```
<Sysname> system-view
[Sysname] ipv6 dhcp guard policy p1
[Sysname-dhcp6-guard-policy-p1] preference max 100 min 1
```

Related commands

ipv6 dhcp server

trust port

Use **trust port** to configure the port to which the DHCPv6 guard policy applies as a trusted port for the policy.

Use **undo trust port** to restore the default.

Syntax

trust port

undo trust port

Default

No trusted port is configured for a DHCPv6 guard policy.

Views

DHCPv6 guard policy view

Predefined user roles

network-admin

Usage guidelines

After you configure this command for a DHCPv6 guard policy, the interface and all interfaces in the VLAN to which the DHCPv6 guard policy is applied are trusted ports. The device forwards received DHCP replies on the trusted ports without check.

The **trust port** command has a higher priority than the **device-role** command. If you configure both commands for a DHCPv6 guard policy, the **trust port** command takes effect.

Examples

Configure the port as a trusted port for the DHCPv6 guard policy.

```
<Sysname> system-view
[Sysname] ipv6 dhcp guard policy p1
```

```
[Sysname-dhcp6-guard-policy-p1] trust port
```

Contents

IPv6 fast forwarding commands

display ipv6 fast-forwarding aging-time

Use **display ipv6 fast-forwarding aging-time** to display the aging time of IPv6 fast forwarding entries.

Syntax

display ipv6 fast-forwarding aging-time

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the aging time of IPv6 fast forwarding entries.

```
<Sysname> display ipv6 fast-forwarding aging-time
Aging time: 30s
```

Table 1 Command output

Field	Description
Aging time	Aging time of IPv6 fast forwarding entries, in seconds.

Related commands

ipv6 fast-forwarding aging-time

display ipv6 fast-forwarding cache

Use **display ipv6 fast-forwarding cache** to display IPv6 fast forwarding entries.

Syntax

display ipv6 fast-forwarding cache [*ipv6-address*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6-address: Specifies an IPv6 address. If you do not specify an IPv6 address, this command displays all IPv6 fast forwarding entries.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 fast forwarding entries for all member devices.

Examples

Display all IPv6 fast forwarding entries.

```
<Sysname> display ipv6 fast-forwarding cache
Total number of IPv6 fast-forwarding items: 2
Src IP: 123::2                                          Src Port: 1036
Dst IP: 123::1                                          Dst Port: 32768
Protocol: 58
VPN instance: N/A
Input interface: Vlan2
Output interface: InLoop0

Src IP: 123::1                                          Src Port: 1036
Dst IP: 123::2                                          Dst Port: 33024
Protocol: 58
VPN instance: N/A
Input interface: InLoop0
Output interface: Vlan2
```

Table 2 Command output

Field	Description
Total number of IPv6 fast-forwarding items	Number of IPv6 fast forwarding entries.
Src IP	Source IPv6 address.
Src port	Source port number.
Dst IP	Destination IPv6 address.
Dst Port	Destination port number.
Protocol	Protocol number.
VPN instance	This field is not supported in the current software version. VPN instance. If the entry does not belong to any VPN instance, this field displays **N/A**.
Input interface	Input interface type and number. If no interface is involved in fast forwarding, this field displays **N/A**. If the input interface does not exist, this field displays a hyphen (-).
Output interface	Output interface type and number. If no interface is involved in fast forwarding, this field displays **N/A**. If the output interface does not exist, this field displays a hyphen (-).

Related commands

`reset ipv6 fast-forwarding cache`

ipv6 fast-forwarding aging-time

Use **`ipv6 fast-forwarding aging-time`** to set the aging time for IPv6 fast forwarding entries.

Use **undo ipv6 fast-forwarding aging-time** to restore the default.

Syntax

ipv6 fast-forwarding aging-time *aging-time*

undo ipv6 fast-forwarding aging-time

Default

The aging time is 30 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

aging-time: Sets the aging time in the range of 10 to 300 seconds.

Examples

Set the aging time to 20 seconds for IPv6 fast forwarding entries.

```
<Sysname> system-view
[Sysname] ipv6 fast-forwarding aging-time 20
```

Related commands

display ipv6 fast-forwarding aging-time

ipv6 fast-forwarding load-sharing

Use **ipv6 fast-forwarding load-sharing** to enable IPv6 fast forwarding load sharing.

Use **undo ipv6 fast-forwarding load-sharing** to disable IPv6 fast forwarding load sharing.

Syntax

ipv6 fast-forwarding load-sharing

undo ipv6 fast-forwarding load-sharing

Default

IPv6 fast forwarding load sharing is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

IPv6 fast forwarding load sharing enables the device to load share packets of the same flow. This feature identifies a data flow by using the packet information.

If IPv6 fast forwarding load sharing is disabled, the device identifies a data flow by the packet information and the input interface. No load sharing is implemented.

Examples

Enable IPv6 fast forwarding load sharing.

```
<Sysname> system-Views
```

```
[Sysname] ipv6 fast-forwarding load-sharing
```

reset ipv6 fast-forwarding cache

Use **reset ipv6 fast-forwarding cache** to clear the IPv6 fast forwarding table.

Syntax

reset ipv6 fast-forwarding cache [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears the IPv6 fast forwarding table for all member devices.

Examples

Clear the IPv6 fast forwarding table.

```
<Sysname> reset ipv6 fast-forwarding cache
```

Related commands

display ipv6 fast-forwarding cache

Contents

HTTP redirect commands

http-redirect https-port

Use **http-redirect https-port** to specify the HTTPS redirect listening port number.

Use **undo http-redirect https-port** to restore the default.

Syntax

http-redirect https-port *port-number*

undo http-redirect https-port

Default

The HTTPS redirect listening port number is 6654.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies the TCP port number on which the HTTPS redirect service listens for HTTPS requests. The value range for the port number is 1 to 65535.

Usage guidelines

To avoid service unavailability caused by port conflict, do not specify a TCP port number used by a well-known protocol or used by any other service. To display TCP port numbers that have been used by services, use the **display tcp** command.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify 8888 as the HTTPS redirect listening port number.

```
<Sysname> system-view
[Sysname] http-redirect https-port 8888
```

http-redirect ssl-server-policy

Use **http-redirect ssl-server-policy** to associate an SSL server policy with the HTTPS redirect service.

Use **undo http-redirect ssl-server-policy** to restore the default.

Syntax

http-redirect ssl-server-policy *policy-name*

undo http-redirect ssl-server-policy

Default

No SSL server policy is associated with the HTTPS redirect service. The HTTPS redirect service uses a self-assigned certificate and the default SSL parameters.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies an SSL server policy by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

HTTPS redirect is unavailable if the associated SSL server policy does not exist. You can first associate a nonexistent SSL server policy with the HTTPS redirect service and then configure the SSL server policy.

If you change the SSL server policy associated with the HTTPS redirect service, the new policy takes effect immediately.

If you perform this task multiple times, the most recent configuration takes effect.

Examples

Associate SSL server policy **policy1** with the HTTPS redirect service.

```
<Sysname> system-view
[Sysname] http-redirect ssl-server-policy policy1
```

Related commands

ssl server-policy

Contents

NAT commands

NAT is supported only in Release 6328 and later.

display nat session

Use **display nat session** to display NAT sessions.

Syntax

display nat session [{ **source-ip** *source-ip* | **destination-ip** *destination-ip* } *] [**slot** *slot-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

source-ip *source-ip*: Displays NAT sessions for the source IP address specified by the *source-ip* argument. The IP address must be the source IP address of the packet that triggers the session establishment.

destination-ip *destination-ip*: Displays NAT sessions for the destination IP address specified by the *destination-ip* argument. The IP address must be the destination IP address of the packet that triggers the session establishment.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays NAT sessions for all member devices.

verbose: Displays detailed information about NAT sessions. If you do not specify this keyword, this command displays brief information about initiators of NAT sessions.

Usage guidelines

If you do not specify any parameters, this command displays detailed information about initiators of all NAT sessions.

Examples

Display detailed information about NAT session initiators for the specified slot.

```
<Sysname> display nat session
Slot 1:
Initiator:
  Source      IP/port: 5.5.5.5/551
  Destination IP/port: 2.2.2.2/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: Vlan-interface100


Total sessions found: 1
```

Display detailed information about NAT sessions for the specified slot.

```
<Sysname> display nat session verbose
Slot 1:
Initiator:
  Source      IP/port: 5.5.5.5/546
  Destination IP/port: 2.2.2.2/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: Vlan-interface100
Responder:
  Source      IP/port: 2.2.2.2/546
  Destination IP/port: 2.2.2.1/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: Vlan-interface101
State: ICMP_REPLY
Application: OTHER
Start time: 2021-04-13 10:27:23  TTL: 27s
Initiator->Responder:            0 packets          0 bytes
Responder->Initiator:            0 packets          0 bytes

Total sessions found: 1
```

Table 1 Command output

Field	Description
Source IP/port	Source IP address and port number.
Destination IP/port	Destination IP address and port number.
DS-Lite tunnel peer	Destination address of the DS-Lite tunnel interface. If the session does not belong to any DS-Lite tunnel, this field displays a hyphen (-).
VPN instance/VLAN ID/VLL ID	The fields identify the following information: • **VPN instance**—MPLS L3VPN instance to which the session belongs. • **VLAN ID**—VLAN to which the session belongs for Layer 2 forwarding. • **VLL ID**—INLINE to which the session belongs for Layer 2 forwarding. If no VPN instance, VLAN ID, or VLL ID is specified, a hyphen (-) is displayed for the related field.
Protocol	Transport layer protocol type: **DCCP**, **ICMP**, **Raw IP**, **SCTP**, **TCP**, **UDP**, or **UDP-Lite**.
Inbound interface	Input interface.
State	NAT session state.
Application	Application layer protocol type, such as **FTP** and **DNS**. This field displays **OTHER** for the protocol types identified by non-well-known ports.
Start time	Time when the session starts.

TTL	Remaining NAT session lifetime in seconds.
Initiator->Responder	Number of packets and bytes from the initiator to the responder.
Responder->Initiator	Number of packets and bytes from the responder to the initiator.
Total sessions found	Total number of sessions.

Related commands

`reset nat session`

display nat static

Use **`display nat static`** to display static NAT mappings.

Syntax

`display nat static`

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display static NAT mappings.

```
<Sysname> display nat static
Static NAT mappings:
  Totally 1 outbound static NAT mappings.
  IP-to-IP:
    Local IP     : 4.4.4.4
    Global IP    : 5.5.5.5
    Config status: Active

Interfaces enabled with static NAT:
  Totally 1 interfaces enabled with static NAT.
  Interface: Vlan-interface100
    Service card : ---
    Config status: Active
```

Table 2 Command output

Field	Description
Static NAT mappings	Information about static NAT mappings.
Totally *n* outbound static NAT mappings	Total number of inbound static NAT mappings.
IP-to-IP	One-to-one static NAT mapping.
Local IP	Private IP address or address range.
Global IP	Public IP address or address range.

Field	Description
Interfaces enabled with static NAT	Interfaces that are enabled with static NAT.
Totally *n* interfaces enabled with static NAT	Total number of interfaces enabled with static NAT.
Interface	Interface enabled with static NAT.
Service card	Service card that processes NAT traffic. If no service card is specified on the interface, this field displays hyphens (---).
Config status	Status of the static NAT mapping configuration: **Active** or **Inactive**.

Related commands

`nat static`

`nat static enable`

nat static enable

Use **`nat static enable`** to enable static NAT on an interface.

Use **`undo nat static enable`** to disable static NAT on an interface

Syntax

`nat static enable`

`undo nat static enable`

Default

Static NAT is disabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

Static NAT mappings take effect on an interface only after you enable static NAT on the interface.

If you configure modular QoS configuration (MQC) on a device enabled with static NAT, packets that match an ACL rule are sent to the CPU. If the packet IP addresses match a NAT rule, the device generates NAT sessions and performs forwarding in software, which might cause packet loss of established NAT sessions.

Examples

Configure an outbound static NAT mapping between private IP address 192.168.1.1 and public IP address 2.2.2.2, and enable static NAT on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] nat static outbound 192.168.1.1 2.2.2.2
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] nat static enable
```

Related commands

`display nat static`

nat static outbound

nat static outbound

Use **nat static outbound** to configure a mapping for outbound static NAT.

Use **undo nat static outbound** to remove a mapping for outbound static NAT.

Syntax

nat static outbound *local-ip global-ip*

undo nat static outbound *local-ip*

Default

No NAT mappings exist.

Views

System view

Predefined user roles

network-admin

Parameters

local-ip: Specifies a private IP address.

global-ip: Specifies a public IP address.

Usage guidelines

When the source IP address of an outgoing packet matches the *local-ip*, the IP address is translated into the *global-ip*. When the destination IP address of an incoming packet matches the *global-ip*, the destination IP address is translated into the *local-ip*.

Examples

Configure an outbound static NAT mapping between public IP address 2.2.2.2 and private IP address 192.168.1.1.

```
<Sysname> system-view
[Sysname] nat static outbound 192.168.1.1 2.2.2.2
```

Related commands

display nat session

display nat static

nat static enable

reset nat session

Use **reset nat session** to clear NAT sessions.

Syntax

reset nat session [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears NAT sessions for all member devices.

Examples

Clear NAT sessions for the specified slot.

```
<Sysname> reset nat session slot 1
```

Related commands

display nat session

Layer 3—IP Routing Command Reference

This command reference is applicable to the following switches and software versions:

H3C S5120V2-LI switch series (Release 6308P01 and later)
H3C S3100V3-SI switch series (Release 6309P01 and later)
H3C S5110V2 switch series (Release 6310 and later)
H3C S5110V2-SI switch series (Release 6310 and later)
H3C S5000V3-EI switch series (Release 6310 and later)
H3C S5000V5-EI switch series (Release 6319P01 and later)
H3C S5000E-X switch series (Release 6310 and later)
H3C S5130S-LI switch series (Release 6310 and later)
H3C MS4320V2 switch series (Release 6308P01 and later)
H3C MS4320 switch series (Release 6308P01 and later)
H3C MS4300V2 switch series (Release 6308P01 and later)
H3C MS4200 switch series (Release 6310 and later)
H3C WS5810-WiNet switch series (Release 6308P01 and later)
H3C WS5820-WiNet switch series (Release 6308P01 and later)
H3C WAS6000 switch series (Release 6308P01 and later)
H3C S5000X-EI switch series (Release 6329 and later)
H3C MS4320V3 switch series (Release 6329 and later)
H3C S5120V3-SI switch series (Release 6329 and later)
H3C S5120V3-LI switch series (Release 6329 and later)

New H3C Technologies Co., Ltd.
http://www.h3c.com

Software version: Release 63xx
Document version: 6W105-20230524

Preface

This command reference describes the routing configuration commands.

This preface includes the following topics about the documentation:

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Documentation feedback

You can e-mail your comments about product documentation to info@h3c.com.

We appreciate your comments.

Contents

Basic IP routing commands

address-family ipv4

Use **address-family ipv4** to create the RIB IPv4 address family and enter its view, or enter the view of the existing RIB IPv4 address family.

Use **undo address-family ipv4** to delete the RIB IPv4 address family and all settings in the view.

Syntax

address-family ipv4

undo address-family ipv4

Default

No RIB IPv4 address family exists.

Views

RIB view

Predefined user roles

network-admin

Examples

Create the RIB IPv4 address family and enter its view.

```
<Sysname> system-view
[Sysname] rib
[Sysname-rib] address-family ipv4
[Sysname-rib-ipv4]
```

address-family ipv6

Use **address-family ipv6** to create the RIB IPv6 address family and enter its view, or enter the view of the existing RIB IPv6 address family.

Use **undo address-family ipv6** to delete the RIB IPv6 address family and all settings in the view.

Syntax

address-family ipv6

undo address-family ipv6

Default

No RIB IPv6 address family exists.

Views

RIB view

Predefined user roles

network-admin

Examples

Create the RIB IPv6 address family and enter its view.

```
<Sysname> system-view
[Sysname] rib
[Sysname-rib] address-family ipv6
[Sysname-rib-ipv6]
```

display ip routing-table

Use **display ip routing-table** to display routing table information.

Syntax

display ip routing-table [**verbose**]

display ip routing-table [**all-routes**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

all-routes: Displays routing table information for all active routes.

verbose: Displays detailed routing table information, including information about both active and inactive routes. If you do not specify this keyword, the command displays only brief information about active routes.

Usage guidelines

If you do not specify any parameters, the command displays only brief information about all active routes in the IPv4 routing table.

Examples

Display brief information about all active routes in the routing table.

```
<Sysname> display ip routing-table

Destinations : 12        Routes : 12

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
192.168.1.0/24      Direct 0    0            192.168.1.40    Vlan11
192.168.1.0/32      Direct 0    0            192.168.1.40    Vlan11
192.168.1.40/32     Direct 0    0            127.0.0.1       InLoop0
192.168.1.255/32    Direct 0    0            192.168.1.40    Vlan11
224.0.0.0/4         Direct 0    0            0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0            0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
```

Display brief information about all active routes in the routing table.

```
<Sysname> display ip routing-table all-routes

VPN instance: public instance
Destinations : 10        Routes : 10

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
1.1.1.0/24          Static 60   0            192.168.47.4    Vlan11
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
192.168.1.40/32     Direct 0    0            127.0.0.1       InLoop0
224.0.0.0/4         Direct 0    0            0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0            0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
```

Table 1 Command output

Field	Description
VPN instance	The routing table belongs to the public network. This field displays **public instance**.
Destinations	Number of destination addresses.
Routes	Number of routes.
Destination/Mask	Destination address/mask length.
Proto	Protocol that installed the route.
Pre	Preference of the route.
Cost	Cost of the route.
NextHop	Next hop address of the route.
Interface	Output interface for packets to be forwarded along the route.
Summary count	Number of routes.

Display detailed information about all routes in the routing table.

```
<Sysname> display ip routing-table verbose

Destinations : 2        Routes : 2

Destination: 0.0.0.0/32
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                  Age: 08h34m37s
       Cost: 0              Preference: 0
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                 State: Active NoAdv
  OrigTblID: 0x0              OrigVrf: default-vrf
    TableID: 0x2               OrigAs: 0
      NibID: 0x10000000        LastAs: 0
```

```
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x1000c        OrigNextHop: 127.0.0.1
      Label: NULL           RealNextHop: 127.0.0.1
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
  Tunnel ID: Invalid          Interface: InLoopBack0
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A                 PathID: 0x0

Destination: 1.1.1.0/24
   Protocol: Static
 Process ID: 0
  SubProtID: 0x0                   Age: 04h20m37s
       Cost: 0               Preference: 60
      IpPre: N/A             QosLocalID: N/A
        Tag: 0                    State: Active Adv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 0
      NibID: 0x10000003          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x1008c        OrigNextHop: 192.168.47.4
      Label: NULL           RealNextHop: 192.168.47.4
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
  Tunnel ID: Invalid          Interface: Vlan-interface11
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A                 PathID: 0x0
```

Table 2 Command output

Field	Description
Destinations	Number of destination addresses.
Routes	Number of routes.
Destination	Destination address/mask length.
Protocol	Protocol that installed the route.
SubProtID	ID of the subprotocol for routing.
Age	Time for which the route has been in the routing table.
Cost	Cost of the route.
Preference	Preference of the route.
IpPre	IP precedence.
QosLocalID	Local QoS ID.
Tag	Route tag.

Field	Description
State	Route status: • **Active**—Active unicast route. • **Adv**—Route that can be advertised. • **Inactive**—Inactive route. • **NoAdv**—Route that the router must not advertise. • **Vrrp**—Routes generated by VRRP. • **Nat**—Routes generated by NAT. • **TunE**—Tunnel. This state is not supported in the current software version.
OrigTblID	Original routing table ID.
OrigVrf	This field is not supported in the current software version. Original VPN instance that the route belongs to. This field displays **default-vrf** if the route is on the public network.
TableID	ID of the routing table.
OrigAs	Original AS number.
NibID	ID of the next hop.
LastAs	Last AS number.
AttrID	Attribute ID.
Neighbor	Address of the neighbor determined by the routing protocol.
Flags	Flags of the route.
OrigNextHop	Next hop address of the route.
RealNextHop	Real next hop of the route.
BkLabel	Backup label.
BkNexthop	Backup next hop.
SRLabel	Segment routing (SR) label.
BkSRLabel	Backup segment routing (SR) label.
Tunnel ID	This field is not supported in the current software version. Tunnel ID.
Interface	Output interface for packets to be forwarded along the route.
BkTunnel ID	This field is not supported in the current software version. Backup tunnel ID.
BkInterface	Backup output interface.
FtnIndex	Index of the FTN entry.
TrafficIndex	Traffic index in the range of 1 to 64. This field displays **N/A** when the value is invalid.
Connector	This field is not supported in the current software version. BGP connector attribute exchanged between BGP peers along with a VPN IPv4 route. The value of the attribute is the IP address of the remote PE device. The BGP connector attribute is used for MD VPN. This field displays **N/A** if the BGP connector attribute is not supported.
Summary count	Number of routes.
PathID	This field is not supported in the current software version. Add-Path ID of the BGP route.

display ip routing-table acl

Use **display ip routing-table acl** to display information about routes permitted by a basic ACL.

Syntax

display ip routing-table acl *ipv4-acl-number* [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv4-acl-number: Specifies a basic ACL by its number in the range of 2000 to 2999.

verbose: Displays detailed information about all routes permitted by the basic ACL. If you do not specify this keyword, the command displays only brief information about active routes permitted by the basic ACL.

Usage guidelines

If the specified ACL does not exist or has no rules configured, the command displays information about all routes.

Examples

Define basic ACL 2000 and set the route filtering rules.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Sysname-acl-ipv4-basic-2000] rule deny source any
```

Display brief information about active routes permitted by basic ACL 2000.

```
[Sysname-acl-ipv4-basic-2000] display ip routing-table acl 2000

Summary count : 4

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
192.168.1.0/24      Direct 0    0            192.168.1.111   Vlan11
192.168.1.0/32      Direct 0    0            192.168.1.111   Vlan11
192.168.1.111/32    Direct 0    0            127.0.0.1       InLoop0
192.168.1.255/32    Direct 0    0            192.168.1.111   Vlan11
```

For command output, see Table 1.

Display detailed information about all routes permitted by basic ACL 2000.

```
<Sysname> display ip routing-table acl 2000 verbose

Summary count : 4

Destination: 192.168.1.0/24
   Protocol: Direct
 Process ID: 0
```

```
  SubProtID: 0x1                   Age: 04h20m37s
       Cost: 0               Preference: 0
      IpPre: N/A             QosLocalID: N/A
        Tag: 0                    State: Active Adv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 0
      NibID: 0x10000003          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x10080        OrigNextHop: 192.168.1.111
      Label: NULL           RealNextHop: 192.168.1.111
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
  Tunnel ID: Invalid          Interface: Vlan-interface11
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A                 PathID: 0x0

Destination: 192.168.1.0/32
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                   Age: 04h20m37s
       Cost: 0               Preference: 0
      IpPre: N/A             QosLocalID: N/A
        Tag: 0                    State: Active NoAdv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 0
      NibID: 0x10000003          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x1008c        OrigNextHop: 192.168.1.111
      Label: NULL           RealNextHop: 192.168.1.111
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
  Tunnel ID: Invalid          Interface: Vlan-interface11
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A                 PathID: 0x0

Destination: 192.168.1.111/32
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x1                   Age: 04h20m37s
       Cost: 0               Preference: 0
      IpPre: N/A             QosLocalID: N/A
        Tag: 0                    State: Active NoAdv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 0
      NibID: 0x10000000          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
```

```
      Flags: 0x10004        OrigNextHop: 127.0.0.1
      Label: NULL           RealNextHop: 127.0.0.1
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
  Tunnel ID: Invalid          Interface: InLoopBack0
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A                 PathID: 0x0

Destination: 192.168.1.255/32
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                   Age: 04h20m37s
       Cost: 0               Preference: 0
      IpPre: N/A             QosLocalID: N/A
        Tag: 0                    State: Active NoAdv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 0
      NibID: 0x10000003          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x1008c         OrigNextHop: 192.168.1.111
      Label: NULL            RealNextHop: 192.168.1.111
    BkLabel: NULL              BkNextHop: N/A
    SRLabel: NULL              BkSRLabel: NULL
  Tunnel ID: Invalid           Interface: Vlan-interface11
BkTunnel ID: Invalid         BkInterface: N/A
   FtnIndex: 0x0            TrafficIndex: N/A
  Connector: N/A                 PathID: 0x0
```

For command output, see Table 2.

display ip routing-table *ip-address*

Use **display ip routing-table** *ip-address* to display information about routes to a specific destination address.

Use **display ip routing-table** *ip-address1* **to** *ip-address2* to display information about routes to a range of destination addresses.

Syntax

display ip routing-table *ip-address* [*mask-length* | *mask*] [**longer-match**] [**verbose**]

display ip routing-table *ip-address1* **to** *ip-address2* [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ip-address: Specifies a destination IP address in dotted decimal notation.

mask-length: Specifies the mask length, an integer in the range of 0 to 32.

mask: Specifies the IP address mask in dotted decimal notation.

longer-match: Displays the route entry with the longest mask.

ip-address1 **to** *ip-address2*: Specifies a destination IP address range.

verbose: Displays detailed routing table information, including information about both active and inactive routes. If you do not specify this keyword, the command displays brief information about active routes.

Usage guidelines

Executing the command with different parameters yields different outputs.

- **display ip routing-table** *ip-address*
  - The system ANDs the entered destination IP address with the subnet mask in each active route entry.
  - The system ANDs the destination IP address in each active route entry with its own subnet mask.

  If the two operations yield the same result for an entry, the entry is displayed.
- **display ip routing-table** *ip-address mask*
  - The system ANDs the entered destination IP address with the entered subnet mask.
  - The system ANDs the destination IP address in each active route entry with the entered subnet mask.

  If the two operations yield the same result for an entry with a subnet mask not greater than the entered subnet mask, the entry is displayed.
- **display ip routing-table** *ip-address* **longer-match**
  - The system ANDs the entered destination IP address with the subnet mask in each active route entry.
  - The system ANDs the destination IP address in each active route entry with its own subnet mask.

  If the two operations yield the same result for multiple entries, the entry with the longest mask length is displayed.
- **display ip routing-table** *ip-address mask* **longer-match**
  - The system ANDs the entered destination IP address with the entered subnet mask.
  - The system ANDs the destination IP address in each active route entry with the entered subnet mask.

  If the two operations yield the same result for multiple entries with a mask not greater than the entered subnet mask, the entry with the longest mask length is displayed.
- **display ip routing-table** *ip-address1* **to** *ip-address2*

  The system displays active route entries with destinations in the range of *ip-address1*/32 to *ip-address2*/32.

Examples

Display brief information about the routes to the destination IP address 11.0.0.1.

```
<Sysname> display ip routing-table 11.0.0.1

Summary count : 3
```

```
Destination/Mask    Proto  Pre  Cost         NextHop         Interface
11.0.0.0/8          Static 60   0            0.0.0.0         NULL0
11.0.0.0/16         Static 60   0            0.0.0.0         NULL0
11.0.0.0/24         Static 60   0            0.0.0.0         NULL0
```

Display brief information about the routes to the destination IP address 11.0.0.1 and mask length 20.

```
<Sysname> display ip routing-table 11.0.0.1 20

Summary count : 2

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
11.0.0.0/8          Static 60   0            0.0.0.0         NULL0
11.0.0.0/16         Static 60   0            0.0.0.0         NULL0
```

Display brief information about the most specific route to the destination address 11.0.0.1.

```
<Sysname> display ip routing-table 11.0.0.1 longer-match

Summary count : 1

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
11.0.0.0/24         Static 60   0            0.0.0.0         NULL0
```

Display brief information about the most specific route to the destination IP address 11.0.0.1 and mask length 20.

```
<Sysname> display ip routing-table 11.0.0.1 20 longer-match

Summary count : 1

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
11.0.0.0/16         Static 60   0            0.0.0.0         NULL0
```

Display brief information about the routes to destination addresses in the range of 1.1.1.0 to 5.5.5.0.

```
<Sysname> display ip routing-table 1.1.1.0 to 5.5.5.0

Summary count : 4

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
1.1.1.1/32          Direct 0    0            127.0.0.1       InLoop0
2.2.2.0/24          Direct 0    0            2.2.2.1         Vlan2
3.3.3.1/32          Direct 0    0            127.0.0.1       InLoop0
4.4.4.1/32          Direct 0    0            127.0.0.1       InLoop0
```

display ip routing-table prefix-list

Use **display ip routing-table prefix-list** to display routes permitted by an IP prefix list.

Syntax

display ip routing-table prefix-list *prefix-list-name* [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

prefix-list-name: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters.

verbose: Displays detailed information about all routes permitted by the IP prefix list. If you do not specify this keyword, the command displays brief information about active routes permitted by the IP prefix list.

Usage guidelines

If the specified IP prefix list does not exist, the command displays information about all routes.

Examples

Create an IP prefix list named **test** to permit the route 1.1.1.0/24.

```
<Sysname> system-view
[Sysname] ip prefix-list test permit 1.1.1.0 24
```

Display brief information about the active route permitted by the IP prefix list.

```
[Sysname] display ip routing-table prefix-list test

Summary count : 1

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
1.1.1.0/24          Direct 0    0            1.1.1.2         Vlan11
```

For command output, see Table 1.

Display detailed information about all routes permitted by the IP prefix list.

```
[Sysname] display ip routing-table prefix-list test verbose

Summary count : 1

Destination: 1.1.1.0/24
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x1                  Age: 04h20m37s
       Cost: 0              Preference: 0
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                 State: Active Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0x2                OrigAs: 0
      NibID: 0x10000003         LastAs: 0
     AttrID: 0xffffffff       Neighbor: 0.0.0.0
      Flags: 0x1008c        OrigNextHop: 1.1.1.2
      Label: NULL           RealNextHop: 1.1.1.2
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
  Tunnel ID: Invalid          Interface: Vlan-interface11
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
```

```
  Connector: N/A                PathID: 0x0
```

For command output, see Table 2.

display ip routing-table protocol

Use **display ip routing-table protocol** to display information about routes installed by a protocol.

Syntax

display ip routing-table protocol *protocol* [**inactive** | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

protocol: Specifies a routing protocol.

inactive: Displays information about inactive routes. If you do not specify this keyword, the command displays information about both active and inactive routes.

verbose: Displays detailed routing table information. If you do not specify this keyword, the command displays brief routing information.

Examples

Display brief information about direct routes.

```
<Sysname> display ip routing-table protocol direct

Summary count : 9

Direct Routing table status : <Active>
Summary count : 9

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
2.2.2.0/24          Direct 0    0            2.2.2.1         Vlan2
2.2.2.0/32          Direct 0    0            2.2.2.1         Vlan2
2.2.2.2/32          Direct 0    0            127.0.0.1       InLoop0
2.2.2.255/32        Direct 0    0            2.2.2.1         Vlan2
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0

Direct Routing table status : <Inactive>
Summary count : 0
```

Display brief information about static routes.

```
<Sysname> display ip routing-table protocol static
```

```
Summary count : 1

Static Routing table status : <Active>
Summary count : 0

Static Routing table status : <Inactive>
Summary count : 1

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
1.2.3.0/24          Static 60   0            1.2.4.5         Vlan10
```

display ip routing-table statistics

Use **display ip routing-table statistics** to display IPv4 route statistics, including numbers of total routes, routes installed by the protocol, routes marked as deleted, and active routes.

Syntax

display ip routing-table [**all-routes**] **statistics**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

all-routes: Displays IPv4 route statistics for all routes. If you do not specify this keyword, the command also displays IPv4 route statistics for all routes.

Examples

Display IPv4 route statistics for all routes.

```
<Sysname> display ip routing-table statistics

Total prefixes: 15        Active prefixes: 15

Proto      Routes      Active      Added       Deleted
DIRECT     12          12          30          18
STATIC     3           3           5           2
RIP        0           0           0           0
OSPF       0           0           0           0
Total      15          15          35          20
```

Display IPv4 route statistics for all routes.

```
<Sysname> display ip routing-table all-routes statistics

Total prefixes: 11        Active prefixes: 11

Proto      Routes      Active      Added       Deleted
DIRECT     8           8           8           0
STATIC     3           3           5           2
```

```
RIP        0           0           0           0
OSPF       0           0           0           0
Total      11          11          13          2
```

Table 3 Command output

Field	Description
Proto	Protocol that installed the route.
Routes	Number of routes installed by the protocol.
Active	Number of active routes.
Added	Number of routes added to the routing table after the router started up or the routing table was cleared most recently.
Deleted	Number of routes marked as deleted, which will be cleared after a period.
Total	Total number of routes.

display ip routing-table summary

Use **display ip routing-table summary** to display brief routing table information.

Syntax

display ip routing-table summary

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display brief routing table information.

```
<Sysname> display ip routing-table summary

Max ECMP: 1
Max Active Route: 1024
Remain Active Route: 1008
```

Table 4 Command output

Field	Description
Max ECMP	ECMP routes are not supported in the current software version. Maximum number of ECMP routes supported by the system.
Max Active Route	Maximum number of supported routes.
Remain Active Route	Number of the remaining inactive routes.

display ipv6 rib graceful-restart

Use **display ipv6 rib graceful-restart** to display IPv6 RIB GR state information.

Syntax

display ipv6 rib graceful-restart

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display IPv6 RIB GR state information.

```
<Sysname> display ipv6 rib graceful-restart
RIB GR state     : Phase2-calculation end
RCOM GR state    : Flush end
Protocol GR state:
 No.  Protocol   Lifetime FD   State    Start/End
-------------------------------------------------
 1    DIRECT     480      29   End      No/No
 2    STATIC     480      32   End      No/No
```

For command output, see Table 9.

display ipv6 rib nib

Use **display ipv6 rib nib** to display next hop information in the IPv6 RIB.

Syntax

display ipv6 rib nib [**self-originated**] [*nib-id*] [**verbose**]

display ipv6 rib nib protocol *protocol* [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

self-originated: Displays information about next hops of self-originated routes in the IPv6 RIB.

nib-id: Specifies a NIB by its ID, a hexadecimal string in the range of 1 to ffffffff.

verbose: Displays detailed next hop information in the IPv6 RIB. If you do not specify this keyword, the command displays brief next hop information in the IPv6 RIB.

protocol *protocol*: Specifies a protocol by its name.

Examples

Display brief next hop information in the IPv6 RIB.

```
<Sysname> display ipv6 rib nib
Total number of nexthop(s): 151

      NibID: 0x20000000        Sequence: 0
```

```
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: ::
    IFIndex: 0x111            LocalAddr: ::
   TopoNthp: Invalid            ExtType: 0x0

      NibID: 0x20000001        Sequence: 1
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: ::1
    IFIndex: 0x112            LocalAddr: ::1
   TopoNthp: Invalid            ExtType: 0x0

...
```

Display detailed next hop information in the IPv6 RIB.

```
<Sysname> display ipv6 rib nib verbose
Total number of nexthop(s): 151

      NibID: 0x20000000        Sequence: 0
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: ::
    IFIndex: 0x111            LocalAddr: ::
   TopoNthp: Invalid            ExtType: 0x0
     RefCnt: 4              FlushRefCnt: 1
       Flag: 0x84               Version: 1
 1 nexthop(s):
PrefixIndex: 0              OrigNexthop: ::
  RelyDepth: 0              RealNexthop: ::
  Interface: NULL0            LocalAddr: ::
  TunnelCnt: 0                      Vrf: default-vrf
   TunnelID: N/A               Topology:
     Weight: 0

      NibID: 0x20000001        Sequence: 1
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: ::1
    IFIndex: 0x112            LocalAddr: ::1
   TopoNthp: Invalid            ExtType: 0x0
     RefCnt: 4              FlushRefCnt: 1
       Flag: 0x84               Version: 1
 1 nexthop(s):
PrefixIndex: 0              OrigNexthop: ::1
  RelyDepth: 0              RealNexthop: ::1
  Interface: InLoop0          LocalAddr: ::1
  TunnelCnt: 0                      Vrf: default-vrf
   TunnelID: N/A               Topology:
```

```
     Weight: 0

       NibID: 0x26000001        Sequence: 1
        Type: 0x1                Flushed: Yes
   UserKey0: 0x0                 VrfNthp: 0
   UserKey1: 0x0                 Nexthop: 121::2
    IFIndex: 0x112             LocalAddr: ::
   TopoNthp: Invalid             ExtType: 0x0
   Instance: default

       NibID: 0x26000002        Sequence: 1
        Type: 0x1                Flushed: Yes
   UserKey0: 0x0                 VrfNthp: 0
   UserKey1: 0x0                 Nexthop: 122::2
    IFIndex: 0x112             LocalAddr: ::
   TopoNthp: Invalid             ExtType: 0x0
   Instance: abc

...
```

For command output, see Table 10 and Table 11.

display ipv6 route-direct nib

Use **display ipv6 route-direct nib** to display next hop information for IPv6 direct routes.

Syntax

display ipv6 route-direct nib [*nib-id*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

nib-id: Specifies a NIB by its ID, a hexadecimal string in the range of 1 to ffffffff.

verbose: Displays detailed next hop information for IPv6 direct routes. If you do not specify this keyword, the command displays brief next hop information for IPv6 direct routes.

Examples

Display brief next hop information for IPv6 direct routes.

```
<Sysname> display ipv6 route-direct nib
Total number of nexthop(s): 115

       NibID: 0x20000000        Sequence: 0
        Type: 0x1                Flushed: Yes
   UserKey0: 0x0                 VrfNthp: 0
   UserKey1: 0x0                 Nexthop: ::
    IFIndex: 0x111             LocalAddr: ::
```

```
   TopoNthp: Invalid            ExtType: 0x0

      NibID: 0x20000001        Sequence: 1
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: ::1
    IFIndex: 0x112            LocalAddr: ::1
   TopoNthp: Invalid            ExtType: 0x0

...
```

Display detailed next hop information for IPv6 direct routes.

```
<Sysname> display ipv6 route-direct nib verbose
Total number of nexthop(s): 115

      NibID: 0x20000000        Sequence: 0
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: ::
    IFIndex: 0x111            LocalAddr: ::
   TopoNthp: Invalid            ExtType: 0x0
     RefCnt: 1              FlushRefCnt: 0
       Flag: 0x2                Version: 1
 1 nexthop(s):
PrefixIndex: 0              OrigNexthop: ::
  RelyDepth: 0              RealNexthop: ::
  Interface: NULL0            LocalAddr: ::
  TunnelCnt: 0                      Vrf: default-vrf
   TunnelID: N/A               Topology:
     Weight: 0

      NibID: 0x20000001        Sequence: 1
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: ::1
    IFIndex: 0x112            LocalAddr: ::1
   TopoNthp: Invalid            ExtType: 0x0
     RefCnt: 1              FlushRefCnt: 0
       Flag: 0x2                Version: 1
 1 nexthop(s):
PrefixIndex: 0              OrigNexthop: ::1
  RelyDepth: 0              RealNexthop: ::1
  Interface: InLoop0          LocalAddr: ::1
  TunnelCnt: 0                      Vrf: default-vrf
   TunnelID: N/A               Topology:
     Weight: 0

...
```

For command output, see Table 12 and Table 13.

display ipv6 routing-table

Use **display ipv6 routing-table** to display IPv6 routing table information.

Syntax

display ipv6 routing-table [**verbose**]

display ipv6 routing-table [**all-routes**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

all-routes: Displays IPv6 routing table information for all active routes.

verbose: Displays detailed routing table information, including information about both active and inactive routes. If you do not specify this keyword, the command displays only brief information about active routes.

Usage guidelines

If you do not specify any parameters, the command displays only brief information about all active routes in the IPv6 routing table.

Examples

Display brief information about all active routes in the IPv6 routing table.

```
<Sysname> display ipv6 routing-table

Destinations : 2 Routes : 2

Destination: ::1/128                                Protocol  : Direct
NextHop    : ::1                                    Preference: 0
Interface  : InLoop0                                Cost      : 0

Destination: FE80::/10                              Protocol  : Direct
NextHop    : ::                                     Preference: 0
Interface  : InLoop0                                Cost      : 0
```

Display brief information about all active routes in the IPv6 routing table.

```
<Sysname> display ipv6 routing-table all-routes

VPN instance: public instance
Destinations : 2 Routes : 2

Destination: ::1/128                                Protocol  : Direct
NextHop    : ::1                                    Preference: 0
Interface  : InLoop0                                Cost      : 0

Destination: FE80::/10                              Protocol  : Direct
NextHop    : ::                                     Preference: 0
```

```
Interface  : InLoop0                                  Cost      : 0
```

Table 5 Command output

Field	Description
VPN instance	The IPv6 routing table belongs to the public network. This field displays **public instance**.
Destinations	Number of destination addresses.
Routes	Number of routes.
Destination	IPv6 address and prefix of the destination network or host.
NextHop	Next hop address of the route.
Preference	Preference of the route.
Interface	Output interface for packets to be forwarded along the route.
Protocol	Protocol that installed the route.
Cost	Cost of the route.
Summary count	Number of routes.

Display detailed information about all routes in the IPv6 routing table.

```
<Sysname> display ipv6 routing-table verbose

Destinations : 2 Routes : 2

Destination: ::1/128
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                  Age: 19h23m02s
       Cost: 0              Preference: 0
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                 State: Active NoAdv
  OrigTblID: 0x0              OrigVrf: default-vrf
    TableID: 0xa               OrigAs: 0
      NibID: 0x20000000        LastAs: 0
     AttrID: 0xffffffff       Neighbor: ::
      Flags: 0x10004       OrigNextHop: ::1
      Label: NULL          RealNextHop: ::1
    BkLabel: NULL            BkNextHop: N/A
    SRLabel: NULL            BkSRLabel: NULL
  Tunnel ID: Invalid         Interface: InLoopBack0
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A                PathID: 0x0

Destination: 12::/96
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                  Age: 00h01m47s
       Cost: 0              Preference: 0
```

```
      IpPre: N/A              QosLocalID: N/A
        Tag: 0                     State: Active Adv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0xa                 OrigAs: 0
      NibID: 0x20000003          LastAs: 0
     AttrID: 0xffffffff        Neighbor: ::
      Flags: 0x10080        OrigNextHop: ::
      Label: NULL           RealNextHop: ::
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
  Tunnel ID: Invalid            Interface: Vlan-interface11
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A                 PathID: 0x0
```

Table 6 Command output

Field	Description
Destination	IPv6 address and prefix of the destination network or host.
Protocol	Protocol that installed the route.
SubProtID	ID of the subprotocol for routing.
Age	Time for which the route has been in the routing table.
Cost	Cost of the route.
Preference	Preference of the route.
IpPre	IP precedence.
QosLocalID	Local QoS ID.
Tag	Tag of the route.
State	Route status: • **Active**—Active unicast route. • **Adv**—Route that can be advertised. • **Inactive**—Inactive route. • **NoAdv**—Route that the router must not advertise. • **Vrrp**—Routes generated by VRRP. • **Nat**—Routes generated by NAT. • **TunE**—Tunnel. This state is not supported in the current software version.
OrigTblID	Original routing table ID.
OrigVrf	This field is not supported in the current software version. Original VPN instance that the route belongs to. This field displays **default-vrf** if the route is on the public network.
TableID	ID of the routing table.
OrigAs	Original AS number.
NibID	ID of the next hop.
LastAs	Last AS number.
AttrID	Attribute ID.
Neighbor	Address of the neighbor determined by the routing protocol.

Field	Description
Flags	Flags of the route.
OrigNextHop	Next hop address of the route.
RealNextHop	Real next hop of the route.
BkLabel	Backup label.
BkNexthop	Backup next hop.
SRLabel	SR label.
BkSRLabel	Backup SR label.
Tunnel ID	This field is not supported in the current software version. Tunnel ID.
Interface	Output interface for packets to be forwarded along the route.
BkTunnel ID	This field is not supported in the current software version. Backup tunnel ID.
BkInterface	Backup output interface.
FtnIndex	Index of the FTN entry.
TrafficIndex	Traffic index in the range of 1 to 64. This field displays **N/A** when the value is invalid.
Connector	This field is not supported in the current software version. BGP connector attribute exchanged between BGP peers along with a VPN IPv4 route. The value of the attribute is the IP address of the remote PE device. The BGP connector attribute is used for MD VPN. This field displays **N/A** if BGP connector attribute is not supported.
Summary count	Number of routes.
PathID	This field is not supported in the current software version. Add-Path ID of the BGP route.

display ipv6 routing-table acl

Use **display ipv6 routing-table acl** to display routing information permitted by an IPv6 basic ACL.

Syntax

display ipv6 routing-table acl *ipv6-acl-number* [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6-acl-number: Specifies a basic IPv6 ACL by its number in the range of 2000 to 2999.

verbose: Displays detailed information about all routes permitted by the basic IPv6 ACL. If you do not specify this keyword, the command displays only brief information about active routes permitted by the basic IPv6 ACL.

Usage guidelines

If the specified IPv6 ACL does not exist or has no rules configured, the command displays information about all IPv6 routes.

Examples

Display brief information about active routes permitted by IPv6 ACL 2000.

```
<Sysname> display ipv6 routing-table acl 2000

Summary count : 6

Destination : ::1/128                                   Protocol  : Direct
NextHop     : ::1                                       Preference: 0
Interface   : InLoop0                                   Cost      : 0

Destination: 12::/96                                    Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : Vlan11                                     Cost      : 0

Destination: 12::1/128                                  Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: 11::1/128                                  Protocol  : O_INTER
NextHop    : FE80::A1F:3FFF:FE45:206                    Preference: 10
Interface  : Vlan11                                     Cost      : 2

Destination: FE80::/10                                  Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: FF00::/8                                   Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : NULL0                                      Cost      : 0
```

For command output, see Table 5.

Display detailed information about all routes permitted by IPv6 ACL 2000.

```
<Sysname> display ipv6 routing-table acl 2000 verbose

Summary count : 6

Destination: ::1/128
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                  Age: 19h29m12s
       Cost: 0              Preference: 0
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                 State: Active NoAdv
  OrigTblID: 0x0              OrigVrf: default-vrf
    TableID: 0xa               OrigAs: 0
```

```
      NibID: 0x20000000          LastAs: 0
     AttrID: 0xffffffff        Neighbor: ::
      Flags: 0x10004        OrigNextHop: ::1
      Label: NULL           RealNextHop: ::1
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
  Tunnel ID: Invalid          Interface: InLoopBack0
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0            TrafficIndex: N/A
  Connector: N/A                PathID: 0x0

Destination: 12::/96
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                   Age: 00h07m57s
       Cost: 0               Preference: 0
      IpPre: N/A             QosLocalID: N/A
        Tag: 0                    State: Active Adv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0xa                 OrigAs: 0
      NibID: 0x20000003          LastAs: 0
     AttrID: 0xffffffff        Neighbor: ::
      Flags: 0x10080        OrigNextHop: ::
      Label: NULL           RealNextHop: ::
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
  Tunnel ID: Invalid          Interface: Vlan-interface11
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0            TrafficIndex: N/A
  Connector: N/A                PathID: 0x0

Destination: 12::1/128
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                   Age: 00h07m55s
       Cost: 0               Preference: 0
      IpPre: N/A             QosLocalID: N/A
        Tag: 0                    State: Active NoAdv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0xa                 OrigAs: 0
      NibID: 0x20000000          LastAs: 0
     AttrID: 0xffffffff        Neighbor: ::
      Flags: 0x10004        OrigNextHop: ::1
      Label: NULL           RealNextHop: ::1
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
  Tunnel ID: Invalid          Interface: InLoopBack0
BkTunnel ID: Invalid        BkInterface: N/A
```

```
   FtnIndex: 0x0          TrafficIndex: N/A
  Connector: N/A                PathID: 0x0

Destination: 11::1/128
   Protocol: O_INTER
 Process ID: 1
  SubProtID: 0x2                  Age: 00h06m43s
       Cost: 2              Preference: 10
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                   State: Active Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0xa                OrigAs: 0
      NibID: 0x23000003         LastAs: 0
     AttrID: 0x ffffffff       Neighbor: ::
      Flags: 0x10041        OrigNextHop: FE80::A1F:3FFF:FE45:206
      Label: NULL           RealNextHop: FE80::A1F:3FFF:FE45:206
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
  Tunnel ID: Invalid          Interface: Vlan-interface11
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0          TrafficIndex: N/A
  Connector: N/A                PathID: 0x0

Destination: FE80::/10
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                  Age: 19h29m12s
       Cost: 0              Preference: 0
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                   State: Active NoAdv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0xa                OrigAs: 0
      NibID: 0x20000002         LastAs: 0
     AttrID: 0xffffffff        Neighbor: ::
      Flags: 0x10084        OrigNextHop: ::
      Label: NULL           RealNextHop: ::
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
  Tunnel ID: Invalid          Interface: InLoopBack0
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0          TrafficIndex: N/A
  Connector: N/A                PathID: 0x0

Destination: FF00::/8
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                  Age: 19h29m12s
       Cost: 0              Preference: 0
```

```
      IpPre: N/A             QosLocalID: N/A
        Tag: 0                    State: Active NoAdv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0xa                 OrigAs: 0
      NibID: 0x20000001          LastAs: 0
     AttrID: 0xffffffff        Neighbor: ::
      Flags: 0x10014        OrigNextHop: ::
      Label: NULL           RealNextHop: ::
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
  Tunnel ID: Invalid          Interface: NULL0
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A                 PathID: 0x0
```

For command output, see Table 6.

display ipv6 routing-table *ipv6-address*

Use **display ipv6 routing-table** *ipv6-address* to display information about routes to an IPv6 destination address.

Use **display ipv6 routing-table** *ipv6-address1* **to** *ipv6-address2* to display information about routes to a range of IPv6 destination addresses.

Syntax

display ipv6 routing-table *ipv6-address* [*prefix-length*] [**longer-match**] [**verbose**]

display ipv6 routing-table *ipv6-address1* **to** *ipv6-address2* [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6-address: Specifies a destination IPv6 address.

prefix-length: Specifies the prefix length in the range of 0 to 128.

longer-match: Displays the route entry with the longest prefix.

ipv6-address1 **to** *ipv6-address2*: Specifies a destination IPv6 address range.

verbose: Displays detailed routing table information, including information about both active and inactive routes. If you do not specify this keyword, the command displays only brief information about active routes.

Usage guidelines

Executing the command with different parameters yields different output.

- **display ipv6 routing-table** *ipv6-address*
  - The system ANDs the entered destination IPv6 address with the prefix length in each active route entry.

- The system ANDs the destination IPv6 address in each active route entry with the prefix length in the entry.

If the two operations yield the same result for an entry, the entry is displayed.

- **display ipv6 routing-table** *ipv6-address prefix-length*
  - The system ANDs the entered destination IPv6 address with the entered prefix length.
  - The system ANDs the destination IPv6 address in each active route entry with the entered prefix length.

  If the two operations yield the same result for an entry with a prefix length not greater than the entered prefix length, the entry is displayed.
- **display ipv6 routing-table** *ipv6-address* **longer-match**
  - The system ANDs the entered destination IPv6 address with the prefix length in each active route entry.
  - The system ANDs the destination IPv6 address in each active route entry with the prefix length in the entry.

  If the two operations yield the same result for multiple entries, the entry with the longest prefix length is displayed.
- **display ipv6 routing-table** *ipv6-address prefix-length* **longer-match**
  - The system ANDs the entered destination IPv6 address with the entered prefix length.
  - The system ANDs the destination IPv6 address in each active route entry with the entered prefix length.

  If the two operations yield the same result for multiple entries with a prefix length not greater than the entered prefix length, the entry with the longest prefix length is displayed.
- **display ipv6 routing-table** *ipv6-address1* **to** *ipv6-address2*

  The system displays route entries with destinations in the range of *ipv6-address1*/128 to *ipv6-address2*/128.

Examples

Display brief information about the routes to the destination IPv6 address 10::1 127.

```
<Sysname> display ipv6 routing-table 10::1 127

Summary count: 3

Destination: 10::/64                                  Protocol  : Static
NextHop    : ::                                       Preference: 60
Interface  : NULL0                                    Cost      : 0

Destination: 10::/68                                  Protocol  : Static
NextHop    : ::                                       Preference: 60
Interface  : NULL0                                    Cost      : 0

Destination: 10::/120                                 Protocol  : Static
NextHop    : ::                                       Preference: 60
Interface  : NULL0                                    Cost      : 0
```

Display brief information about the most specific route to the destination IPv6 address 10::1 and prefix length 127.

```
<Sysname> display ipv6 routing-table 10::1 127 longer-match

Summary count : 1
```

```
Destination: 10::/120                                   Protocol  : Static
NextHop    : ::                                         Preference: 60
Interface  : NULL0                                      Cost      : 0
```

Display brief information about the routes to destination addresses in the range of 100:: to 300::.

```
<Sysname> display ipv6 routing-table 100:: to 300::

Summary count : 3

Destination: 100::/64                                   Protocol  : Static
NextHop    : ::                                         Preference: 60
Interface  : NULL0                                      Cost      : 0

Destination: 200::/64                                   Protocol  : Static
NextHop    : ::                                         Preference: 60
Interface  : NULL0                                      Cost      : 0

Destination: 300::/64                                   Protocol  : Static
NextHop    : ::                                         Preference: 60
Interface  : NULL0                                      Cost      : 0
```

Display detailed information about the routes to destination IPv6 addresses 1:2::3:4/128.

```
<Sysname> display ipv6 routing-table 1:2::3:4 128 verbose

Summary count : 1

Destination: 1:2::3:4/128
   Protocol: O_INTRA
 Process ID: 1
  SubProtID: 0x1                  Age: 00h01m14s
       Cost: 1              Preference: 10
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                 State: Active Adv
  OrigTblID: 0x0              OrigVrf: default-vrf
    TableID: 0xa               OrigAs: 0
      NibID: 0x23000002        LastAs: 0
     AttrID: 0xffffffff       Neighbor: ::
      Flags: 0x10041       OrigNextHop: FE80::A1F:3FFF:FE45:206
      Label: NULL          RealNextHop: FE80::A1F:3FFF:FE45:206
    BkLabel: NULL            BkNextHop: N/A
    SRLabel: NULL            BkSRLabel: NULL
  Tunnel ID: Invalid           Interface: Vlan-interface11
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A                PathID: 0x0
```

For command output, see Table 5.

display ipv6 routing-table prefix-list

Use **display ipv6 routing-table prefix-list** to display information about IPv6 routes permitted by an IPv6 prefix list.

Syntax

display ipv6 routing-table prefix-list *prefix-list-name* [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

prefix-list-name: Specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters.

verbose: Displays detailed information about all IPv6 routes permitted by the IPv6 prefix list. If you do not specify this keyword, the command displays brief information about active IPv6 routes permitted by the IPv6 prefix list.

Usage guidelines

If the specified IPv6 prefix list does not exist, the command displays information about all routes.

Examples

Create an IPv6 prefix list named test to permit the prefix ::1/128.

```
<Sysname> system-view
[Sysname] ipv6 prefix-list test permit ::1 128
```

Display brief information about the active IPv6 route permitted by the IPv6 prefix list.

```
[Sysname] display ipv6 routing-table prefix-list test

Summary count : 1

Destination: ::1/128                                Protocol  : Direct
NextHop    : ::1                                    Preference: 0
Interface  : InLoop0                                Cost      : 0
```

For command output, see Table 5.

Display detailed information about all routes permitted by the IPv6 prefix list.

```
[Sysname] display ipv6 routing-table prefix-list test verbose

Summary count : 1

Destination: ::1/128
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                    Age: 08h57m19s
       Cost: 0               Preference: 0
      IpPre: N/A             QosLocalID: N/A
        Tag: 0                    State: Active NoAdv
```

```
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0xa                 OrigAs: 0
      NibID: 0x20000000          LastAs: 0
     AttrID: 0xffffffff        Neighbor: ::
      Flags: 0x10004        OrigNextHop: ::1
      Label: NULL           RealNextHop: ::1
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
  Tunnel ID: Invalid          Interface: InLoopBack0
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A                 PathID: 0x0
```

For command output, see Table 6.

display ipv6 routing-table protocol

Use **display ipv6 routing-table protocol** to display information about IPv6 routes installed by a protocol.

Syntax

display ipv6 routing-table protocol *protocol* [**inactive** | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

protocol: Specifies a routing protocol.

inactive: Displays information about inactive routes. If you do not specify this keyword, the command displays information about both active and inactive routes.

verbose: Displays detailed routing table information. If you do not specify this keyword, the command displays brief routing information.

Examples

Display brief information about IPv6 direct routes.

```
<Sysname> display ipv6 routing-table protocol direct

Summary count : 3

Direct Routing table status : <Active>
Summary count : 3

Destination: ::1/128                                Protocol  : Direct
NextHop    : ::1                                    Preference: 0
Interface  : InLoop0                                Cost      : 0

Destination: FE80::/10                              Protocol  : Direct
```

```
NextHop    : ::                                    Preference: 0
Interface  : InLoop0                               Cost      : 0

Destination: FF00::/8                              Protocol  : Direct
NextHop    : ::                                    Preference: 0
Interface  : NULL0                                 Cost      : 0

Direct Routing table status : <Inactive>
Summary count : 0
```

Display brief information about IPv6 static routes.

```
<Sysname> display ipv6 routing-table protocol static

Summary count : 3

Static Routing table status : <Active>
Summary count : 3

Destination: 2::2/128                              Protocol  : Static
NextHop    : fe80::2                               Preference: 60
Interface  : Vlan12                                Cost      : 0

Destination: 2::2/128                              Protocol  : Static
NextHop    : fe80::3                               Preference: 60
Interface  : Vlan12                                Cost      : 0

Destination: 3::3/128                              Protocol  : Static
NextHop    : 2::2                                  Preference: 60
Interface  : Vlan12                                Cost      : 0

Static Routing table status : <Inactive>
Summary count : 0
```

display ipv6 routing-table statistics

Use **display ipv6 routing-table statistics** to display IPv6 route statistics, including numbers of total routes, routes installed and deleted by the protocol, and active routes.

Syntax

display ipv6 routing-table [**all-routes**] **statistics**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

all-routes: Displays IPv6 route statistics for all routes. If you do not specify this keyword, the command also displays IPv6 route statistics for all routes.

Examples

Display IPv6 route statistics.

```
<Sysname> display ipv6 routing-table statistics

Total prefixes: 8        Active prefixes: 8

Proto      Routes      Active      Added       Deleted
DIRECT     5           5           5           0
STATIC     3           3           3           0
RIPng      0           0           0           0
OSPFv3     0           0           0           0
Total      8           8           8           0
```

Display IPv6 route statistics.

```
<Sysname> display ipv6 routing-table all-routes statistics

Total prefixes: 6        Active prefixes: 6

Proto      Routes      Active      Added       Deleted
DIRECT     3           3           3           0
STATIC     3           3           5           2
RIPng      0           0           0           0
OSPFv3     0           0           0           0
Total      6           6           8           2
```

Table 7 Command output

Field	Description
Proto	Protocol that installed the route.
Routes	Number of routes installed by the protocol.
Active	Number of active routes.
Added	Number of routes added to the routing table after the router started up or the routing table was cleared most recently.
Deleted	Number of routes marked as deleted, which will be cleared after a period.
Total	Total number of routes.

display ipv6 routing-table summary

Use **display ipv6 routing-table summary** to display brief IPv6 routing table information.

Syntax

display ipv6 routing-table summary

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display brief IPv6 routing table information.

```
<Sysname> display ipv6 routing-table summary

Max ECMP: 1
Max Active Route: 256
Remain Active Route: 251
```

Table 8 Command output

Field	Description
Max ECMP	ECMP routes are not supported in the current software version. Maximum number of ECMP routes supported by the system.
Max Active Route	Maximum number of supported routes.
Remain Active Route	Number of the remaining inactive routes.

display rib graceful-restart

Use **`display rib graceful-restart`** to display RIB GR state information.

Syntax

`display rib graceful-restart`

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display RIB GR state information.

```
<Sysname> display rib graceful-restart
RIB GR state     : Phase2-calculation end
RCOM GR state    : Flush end
Protocol GR state:
 No.  Protocol   Lifetime FD   State    Start/End
-------------------------------------------------
 1    DIRECT     100      30   End      No/No
 2    STATIC     480      34   End      No/No
 3    OSPF       480      36   End      No/No
```

Table 9 Command output

Field	Description
RIB GR state	RIB GR status: • **Start**—GR starts. • **IGP end**—All IGP protocols complete GR. • **Routing protocol end**—All routing protocols complete GR. • **NSR-calculation unfinished**—NSR has not finished optimal route selection. • **Triggering start**—All triggered optimal route selection starts. • **Triggering end**—All triggered optimal route selection completes. • **Phase1-calculation end**—Optimal route selection phase 1 completes. • **All end**—All protocols complete GR. • **Phase2-calculation end**—Optimal route selection phase 2 completes.
RCOM GR state	RCOM GR status: • **Start**—GR starts. • **Routing protocol end**—All routing protocols complete GR. • **NSR-calculation unfinished**—NSR has not finished optimal route selection. • **Phase1-calculation end**—Optimal route selection phase 1 completes. • **Notification end**—All routes have been delivered to the route management module. • **Phase2-calculation end**—Optimal route selection phase 2 completes. • **Flush start**—Starts to flush routes to the FIB. • **Flush end**—Completes flushing routes to the FIB.
No.	Protocol number.
Lifetime	Lifetime (in seconds) of routes/labels in the RIB during GR.
FD	Handle between the protocol and the RIB.
State	Protocol GR state: • **Init**—Initialization state. • **Listen**—Listening state. • Idle. • Active. • **Start**—GR starts. • **End**—GR completes.
Start/End	Message sending state: • **No**—The message has not been sent. • **Yes**—The message has been sent.

display rib nib

Use **display rib nib** to display next hop information in the RIB.

Syntax

display rib nib [**self-originated**] [*nib-id*] [**verbose**]

display rib nib protocol *protocol* [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

`self-originated`: Displays information about next hops of self-originated routes in the RIB.

`nib-id`: Specifies a NIB by its ID, a hexadecimal string in the range of 1 to ffffffff.

`verbose`: Displays detailed next hop information in the RIB. If you do not specify this keyword, the command displays brief next hop information in the RIB.

`protocol` *`protocol`*: Specifies a protocol by its name.

Examples

Display brief next hop information in the RIB.

```
<Sysname> display rib nib
Total number of nexthop(s): 176

      NibID: 0x10000000        Sequence: 0
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 0.0.0.0
    IFIndex: 0x111             LocalAddr: 0.0.0.0
   TopoNthp: 0                  ExtType: 0x0

      NibID: 0x10000001        Sequence: 1
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 127.0.0.1
    IFIndex: 0x112             LocalAddr: 127.0.0.1
   TopoNthp: 0                  ExtType: 0x0

      NibID: 0x10000002        Sequence: 2
       Type: 0x5                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 127.0.0.1
    IFIndex: 0x112             LocalAddr: 127.0.0.1
   TopoNthp: 0                  ExtType: 0x0

      NibID: 0x16000000        Sequence: 3
       Type: 0x21               Flushed: No
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 12.1.1.2
    IFIndex: 0x0               LocalAddr: 0.0.0.0
   TopoNthp: 0                  ExtType: 0x0
   Instance: abc
```

...

Table 10 Command output

Field	Description
NibID	ID of the next hop.
Sequence	Sequence number of the next hop.
Type	Type of the next hop.
Flushed	Indicates whether the route with the next hop has been flushed to the FIB.
UserKey0	Reserved data 1.
UserKey1	Reserved data 2.
VrfNthp	This field is not supported in the current software version. Index of the VPN instance that the next hop belongs to. This field displays **0** if the next hop is on the public network.
Nexthop	Next hop address.
IFIndex	Interface index.
LocalAddr	Local interface address.
TopoNthp	This field is not supported in the current software version. Index of the topology that contains the next hop. This field displays **0** if the next hop is on the IPv4 public network. This field displays **Invalid** if the next hop is on an IPv6 network, because the router does not support multiple IPv6 topologies.
ExtType	Extension type of the next hop.
SubNibID	ID of the sub-next hop.
SubSeq	Sequence number of the sub-next hop.
NthpCnt	Number of sub-next hops.
Samed	Number of the same sub-next hops.
NthpType	Type of the sub-next hop: **IP**—IP forwarding.

Display detailed next hop information in the RIB.

```
<Sysname> display rib nib verbose
Total number of nexthop(s): 176

      NibID: 0x10000000        Sequence: 0
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 0.0.0.0
    IFIndex: 0x111            LocalAddr: 0.0.0.0
   TopoNthp: 0                  ExtType: 0x0
     RefCnt: 6              FlushRefCnt: 2
       Flag: 0x84                Version: 1
 1 nexthop(s):
PrefixIndex: 0              OrigNexthop: 0.0.0.0
  RelyDepth: 0              RealNexthop: 0.0.0.0
  Interface: NULL0            LocalAddr: 0.0.0.0
```

```
  TunnelCnt: 0                    Vrf: default-vrf
   TunnelID: N/A                Topology: base
     Weight: 0

      NibID: 0x10000001        Sequence: 1
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 127.0.0.1
    IFIndex: 0x112             LocalAddr: 127.0.0.1
   TopoNthp: 0                   ExtType: 0x0
     RefCnt: 11               FlushRefCnt: 5
       Flag: 0x84                Version: 1
 1 nexthop(s):
PrefixIndex: 0                OrigNexthop: 127.0.0.1
  RelyDepth: 0                RealNexthop: 127.0.0.1
  Interface: InLoop0            LocalAddr: 127.0.0.1
  TunnelCnt: 0                    Vrf: default-vrf
   TunnelID: N/A                Topology: base
     Weight: 0

      NibID: 0x15000003        Sequence: 3
       Type: 0x43                Flushed: Yes
   UserKey0: 0x100010000         VrfNthp: 0
   UserKey1: 0x0                Nexthop: 22.22.22.22
    IFIndex: 0x0               LocalAddr: 0.0.0.0
   TopoNthp: 0                   ExtType: 0x0
     RefCnt: 9                FlushRefCnt: 3
       Flag: 0x84                Version: 1
     Policy: tnl-policy1
 1 nexthop(s):
PrefixIndex: 0                OrigNexthop: 22.22.22.22
  RelyDepth: 1                RealNexthop: 13.1.1.2
  Interface: Vlan11             LocalAddr: 13.1.1.1
  TunnelCnt: 1                    Vrf: default-vrf
   TunnelID: 1025               Topology: base
     Weight: 0

...
```

Table 11 Command output

Field	Description
NibID	ID of the next hop.
Sequence	Sequence number of the next hop.
Type	Type of the next hop.
Flushed	Indicates whether the route with the next hop has been flushed to the FIB.
UserKey0	Reserved data 1.

Field	Description
UserKey1	Reserved data 2.
VrfNthp	This field is not supported in the current software version. Index of the VPN instance that the next hop belongs to. This field displays **0** if the next hop is on the public network.
Nexthop	Next hop address.
IFIndex	Interface index.
LocalAddr	Local interface address.
TopoNthp	This field is not supported in the current software version. Index of the topology that contains the next hop. This field displays **0** if the next hop is on the IPv4 public network. This field displays **Invalid** if the next hop is on an IPv6 network, because the router does not support multiple IPv6 topologies.
ExtType	Extension type of the next hop.
SubNibID	ID of the sub-next hop.
SubSeq	Sequence number of the sub-next hop.
NthpCnt	Number of sub-next hops.
Samed	Number of the same sub-next hops.
NthpType	Type of the sub-next hop: • **IP**—IP forwarding.
x nexthop (s)	Number of next hops.
PrefixIndex	Prefix index of the next hop for an ECMP route.
Vrf	This field is not supported in the current software version. VPN instance name. For the public network, this field displays **default-vrf**.
OrigNexthop	Original next hop.
RealNexthop	Real next hop.
Interface	Output interface.
LocalAddr	Local interface address.
RelyDepth	Recursion depth.
TunnelCnt	This field is not supported in the current software version. Number of tunnels after route recursion.
TunnelID	This field is not supported in the current software version. ID of the tunnel after route recursion.
Topology	This field is not supported in the current software version. Topology name. The topology name for the IPv4 public network is **base**. This field is blank for IPv6, because IPv6 does not support multiple topologies.
Weight	ECMP routes are not supported in the current software version. ECMP route weight. This field displays 0 for non-ECMP routes.
RefCnt	Reference count of the next hop.
FlushRefCnt	Reference count of the next hop that is flushed to the FIB.
Flag	Flag of the next hop.

Field	Description
Version	Version of the next hop.

display route-direct nib

Use **display route-direct nib** to display next hop information for direct routes.

Syntax

display route-direct nib [*nib-id*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

nib-id: Specifies a NIB by its ID, a hexadecimal string in the range of 1 to ffffffff.

verbose: Displays detailed next hop information for direct routes. If you do not specify this keyword, the command displays brief next hop information for direct routes.

Examples

Display brief next hop information for direct routes.

```
<Sysname> display route-direct nib
Total number of nexthop(s): 116

      NibID: 0x10000000        Sequence: 0
       Type: 0x1                 Flushed: Yes
   UserKey0: 0x0                 VrfNthp: 0
   UserKey1: 0x0                 Nexthop: 0.0.0.0
    IFIndex: 0x111             LocalAddr: 0.0.0.0
   TopoNthp: 0                   ExtType: 0x0

      NibID: 0x10000001        Sequence: 1
       Type: 0x1                 Flushed: Yes
   UserKey0: 0x0                 VrfNthp: 0
   UserKey1: 0x0                 Nexthop: 127.0.0.1
    IFIndex: 0x112             LocalAddr: 127.0.0.1
   TopoNthp: 0                   ExtType: 0x0

...
```

Table 12 Command output

Field	Description
NibID	ID of the NIB.
Sequence	Sequence number of the NIB.

Field	Description
Type	Type of the NIB.
Flushed	Indicates whether the route with the NIB has been flushed to the FIB.
UserKey0	Reserved data 1.
UserKey1	Reserved data 2.
VrfNthp	This field is not supported in the current software version. Index of the VPN instance that the next hop belongs to. This field displays **0** if the next hop is on the public network.
Nexthop	Next hop address.
IFIndex	Interface index.
LocalAddr	Local interface IP address.
TopoNthp	This field is not supported in the current software version. Index of the topology that contains the next hop. This field displays **0** if the next hop is on the IPv4 public network. This field displays **Invalid** if the next hop is on an IPv6 network, because the router does not support multiple IPv6 topologies.
ExtType	Extension type of the next hop.

Display detailed next hop information for direct routes.

```
<Sysname> display route-direct nib verbose
Total number of nexthop(s): 116

      NibID: 0x10000000        Sequence: 0
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 0.0.0.0
    IFIndex: 0x111             LocalAddr: 0.0.0.0
   TopoNthp: 0                   ExtType: 0x0
     RefCnt: 2               FlushRefCnt: 0
       Flag: 0x2                 Version: 1
 1 nexthop(s):
PrefixIndex: 0               OrigNexthop: 0.0.0.0
  RelyDepth: 0               RealNexthop: 0.0.0.0
  Interface: NULL0             LocalAddr: 0.0.0.0
  TunnelCnt: 0                       Vrf: default-vrf
   TunnelID: N/A                Topology: base
     Weight: 0

      NibID: 0x10000001        Sequence: 1
       Type: 0x1                Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 127.0.0.1
    IFIndex: 0x112             LocalAddr: 127.0.0.1
   TopoNthp: 0                   ExtType: 0x0
     RefCnt: 5               FlushRefCnt: 0
       Flag: 0x2                 Version: 1
```

```
 1 nexthop(s):
PrefixIndex: 0              OrigNexthop: 127.0.0.1
  RelyDepth: 0              RealNexthop: 127.0.0.1
  Interface: InLoop0          LocalAddr: 127.0.0.1
  TunnelCnt: 0                      Vrf: default-vrf
   TunnelID: N/A               Topology: base
     Weight: 0
...
```

Table 13 Command output

Field	Description
NibID	ID of the next hop.
Sequence	Sequence number of the next hop.
Type	Type of the next hop.
Flushed	Indicates whether the route with the next hop has been flushed to the FIB.
UserKey0	Reserved data 1.
VrfNthp	This field is not supported in the current software version. Index of the VPN instance to which the next hop belongs. This field displays **0** if the next hop is on the public network.
UserKey1	Reserved data 2.
Nexthop	Next hop address.
IFIndex	Interface index.
LocalAddr	Local interface address.
TopoNthp	This field is not supported in the current software version. Index of the topology that contains the next hop. This field displays **0** if the next hop is on the IPv4 public network. This field displays **Invalid** if the next hop is on an IPv6 network, because the router does not support multiple IPv6 topologies.
ExtType	Extension type of the next hop.
RefCnt	Reference count of the next hop.
FlushRefCnt	Reference count of the next hop that is flushed to the FIB.
Flag	Flag of the next hop.
Version	Version of the next hop.
x nexthop(s)	Number of next hops.
PrefixIndex	Prefix index of the next hop for an ECMP route.
OrigNexthop	Original next hop.
RelyDepth	Recursion depth.
RealNexthop	Real next hop.
Interface	Output interface.
LocalAddr	Local interface address.
TunnelCnt	This field is not supported in the current software version. Number of tunnels after route recursion.

Field	Description
Vrf	This field is not supported in the current software version. VPN instance name. For the public network, this field displays **default-vrf**.
TunnelID	This field is not supported in the current software version. ID of the tunnel after route recursion.
Topology	This field is not supported in the current software version. Topology name. The topology name for the IPv4 public network is **base**. This field is blank for IPv6, because IPv6 does not support multiple topologies.
Weight	ECMP routes are not supported in the current software version. ECMP route weight. This field displays 0 for non-ECMP routes.

fib lifetime

Use **fib lifetime** to set the maximum lifetime for IPv4 or IPv6 routes in the FIB.

Use **undo fib lifetime** to restore the default.

Syntax

fib lifetime *seconds*

undo fib lifetime

Default

The maximum lifetime for IPv4 or IPv6 routes in the FIB is 600 seconds.

Views

RIB IPv4 address family view

RIB IPv6 address family view

Predefined user roles

network-admin

Parameters

seconds: Specifies the maximum lifetime for routes in the FIB, in the range of 0 to 6000 seconds. When this argument is set to 0, FIB entries immediately age out after a protocol or RIB process switchover.

Usage guidelines

When a protocol or RIB process switchover occurs and GR or NSR is not configured, FIB entries age out after the time specified in this command.

Examples

Set the maximum lifetime for IPv4 routes in the FIB to 60 seconds.

```
<Sysname> system-view
[Sysname] rib
[Sysname-rib] address-family ipv4
[Sysname-rib-ipv4] fib lifetime 60
```

inter-protocol fast-reroute

Use **inter-protocol fast-reroute** to enable IPv4 or IPv6 RIB inter-protocol FRR.

Use **undo inter-protocol fast-reroute** to disable IPv4 or IPv6 RIB inter-protocol FRR.

Syntax

inter-protocol fast-reroute

undo inter-protocol fast-reroute

Default

Inter-protocol FRR is disabled.

Views

RIB IPv4 address family view

RIB IPv6 address family view

Predefined user roles

network-admin

Usage guidelines

This command allows a device to perform fast rerouting between routes of different protocols. A backup next hop is automatically selected to reduce the service interruption time caused by unreachable next hops. When the next hop of the primary link fails, the traffic is redirected to the backup next hop.

This command uses the next hop of a route from a different protocol as the backup next hop for the faulty route, which might cause loops.

Inter-protocol FRR cannot select a backup next hop from routes in the RIB that have the same next hop, output interface, and destination as those of the faulty route.

Examples

Enable IPv4 RIB inter-protocol FRR.

```
<Sysname> system-view
[Sysname] rib
[Sysname-rib] address-family ipv4
[Sysname-rib-ipv4] inter-protocol fast-reroute
```

ip route fast-switchover enable

Use **ip route fast-switchover enable** to enable IPv4 route fast switchover.

Use **undo ip route fast-switchover enable** to disable IPv4 route fast switchover.

Syntax

ip route fast-switchover enable

undo ip route fast-switchover enable

Default

IPv4 route fast switchover is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Use this command if a physical interface is the output interface for a large number of routes, including primary/secondary routes. When a link failure occurs on an interface, the device typically performs the following operations before switching the traffic to a valid route:

1. Deletes all ARP entries for the link.
2. Instructs the FIB to delete the associated FIB entries.

This process is time-consuming and interruptive if a large number of routes traverse the interface. Route fast switchover minimizes traffic interruption by instructing the FIB to delete the affected FIB entries immediately without having to wait for the ARP entries to be deleted.

Examples

Enable IPv4 route fast switchover.

```
<Sysname> system-view
[Sysname] ip route fast-switchover enable
```

ipv6 route fast-switchover enable

Use **ipv6 route fast-switchover enable** to enable IPv6 route fast switchover.

Use **undo ipv6 route fast-switchover enable** to disable IPv6 route fast switchover.

Syntax

ipv6 route fast-switchover enable

undo ipv6 route fast-switchover enable

Default

IPv6 route fast switchover is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Use this command if a physical interface is the output interface for a large number of routes, including primary/secondary routes. When a link failure occurs on an interface, the device typically performs the following operations before switching the traffic to a valid route:

1. Deletes all ND entries for the link.
2. Instructs the FIB to delete the associated FIB entries.

This process is time-consuming and interruptive if a large number of routes traverse the interface. Route fast switchover minimizes traffic interruption by instructing the FIB to delete the affected FIB entries immediately without having to wait for the ND entries to be deleted.

Examples

Enable IPv6 route fast switchover.

```
<Sysname> system-view
[Sysname] ipv6 route fast-switchover enable
```

maintenance-probe enable

Use **maintenance-probe enable** to enable maintenance probe (MTP).

Use **undo maintenance-probe enable** to disable MTP.

Syntax

maintenance-probe enable

undo maintenance-probe enable

Default

MTP is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

MTP enables the device to automatically perform the following operations upon expiration of a neighbor's hold timer:

1. Ping the neighbor or trace the route to the neighbor.
2. Record the ping or tracert results.

To view fault information, use the **display** commands of routing protocols, for example, the **display ospf troubleshooting** command. To view detailed MTP information, use the **display logbuffer** command.

Examples

Enable MTP.

```
<Sysname> system-view
[Sysname] maintenance-probe enable
```

non-stop-routing

Use **non-stop-routing** to enable RIB NSR.

Use **undo non-stop-routing** to disable RIB NSR.

Syntax

non-stop-routing

undo non-stop-routing

Default

RIB NSR is disabled.

Views

RIB IPv4 address family view

RIB IPv6 address family view

Predefined user roles

network-admin

Examples

Enable NSR for the RIB IPv4 address family.

```
<Sysname> system-view
[Sysname] rib
[Sysname-rib] address-family ipv4
[Sysname-rib-ipv4] non-stop-routing
```

protocol lifetime

Use **protocol lifetime** to set the maximum lifetime for IPv4 or IPv6 routes and labels in the RIB.

Use **undo protocol lifetime** to restore the default.

Syntax

protocol *protocol* **lifetime** *seconds*

undo protocol *protocol* **lifetime**

Default

The maximum lifetime for IPv4 or IPv6 routes and labels in the RIB is 480 seconds.

Views

RIB IPv4 address family view

RIB IPv6 address family view

Predefined user roles

network-admin

Parameters

protocol: Specifies a routing protocol.

seconds: Specifies the maximum lifetime for routes and labels in the RIB, in the range of 1 to 6000 seconds.

Usage guidelines

When GR is enabled, make sure the protocol can complete GR and install all route entries to the RIB within the lifetime configured in this command.

Examples

Set the maximum lifetime for RIP routes and labels in the RIB to 60 seconds.

```
<Sysname> system-view
[Sysname] rib
[Sysname-rib] address-family ipv4
[Sysname-rib-ipv4] protocol rip lifetime 60
```

protocol nexthop recursive-lookup

Use **protocol nexthop recursive-lookup** to configure routing policy-based recursive lookup.

Use **undo protocol nexthop recursive-lookup** to remove the configuration.

Syntax

protocol *protocol* **nexthop recursive-lookup route-policy** *route-policy-name*

undo protocol *protocol* **nexthop recursive-lookup route-policy**

Default

Routing policy-based recursive lookup is not configured.

Views

RIB IPv4 address family view

Predefined user roles

network-admin

Parameters

protocol: Specifies a routing protocol, which can be **static** in RIB IPv4 address family view.

route-policy-name: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

Configure routing policy-based recursive lookup to control route recursion results. For example, when a route changes, the routing protocol has to perform a route recursion if the next hop is indirectly connected. The routing protocol might select an incorrect path, which can cause traffic loss. To resolve this issue, you can use a routing policy to filter out incorrect routes. The routes that pass the filtering of the routing policy will be used for route recursion.

The **apply** clauses in the specified routing policy cannot take effect.

Make sure a minimum of one related route can match the routing policy for correct traffic forwarding.

Examples

Configure recursive lookup based on routing policy **policy1** for static routes.

```
<Sysname> system-view
[Sysname] rib
[Sysname-rib] address-family ipv4
[Sysname-rib-ipv4] protocol static nexthop recursive-lookup route-policy policy1
```

reset ip routing-table statistics protocol

Use **reset ip routing-table statistics protocol** to clear IPv4 route statistics.

Syntax

reset ip routing-table statistics protocol { *protocol* | **all** }

reset ip routing-table [**all-routes**] **statistics protocol** { *protocol* | **all** }

Views

User view

Predefined user roles

network-admin

Parameters

all-routes: Clears route statistics for all IPv4 routes.

protocol: Clears route statistics for a routing protocol.

all: Clears route statistics for all IPv4 routing protocols.

Usage guidelines

This command clears IPv4 route statistics for all IPv4 routes of the specified routing protocols even if you do not specify the **all-routes** keyword.

This command clears only statistics of added and deleted routes for the specified routing protocols.

Examples

Clear all IPv4 route statistics.

```
<Sysname> reset ip routing-table statistics protocol all
```

reset ipv6 routing-table statistics protocol

Use **reset ipv6 routing-table statistics protocol** to clear IPv6 route statistics.

Syntax

reset ipv6 routing-table statistics protocol { *protocol* | **all** }

reset ipv6 routing-table [**all-routes**] **statistics protocol** { *protocol* | **all** }

Views

User view

Predefined user roles

network-admin

Parameters

all-routes: Clears route statistics for all IPv6 routes.

protocol: Clears route statistics for an IPv6 routing protocol.

all: Clears route statistics for all IPv6 routing protocols.

Usage guidelines

This command clears IPv6 route statistics for all IPv6 routes of the specified routing protocols even if you do not specify the **all-routes** keyword.

This command clears only statistics of added and deleted routes for the specified routing protocols.

Examples

Clear all IPv6 route statistics.

```
<Sysname> reset ipv6 routing-table statistics protocol all
```

rib

Use **rib** to enter RIB view.

Use **undo rib** to remove all configurations in RIB view.

Syntax

rib

undo rib

Views

System view

Predefined user roles

network-admin

Examples

Enter RIB view.

```
<Sysname> system-view
[Sysname] rib
[Sysname-rib]
```

routing-table limit

Use **routing-table limit** to set the maximum number of active IPv4/IPv6 routes supported by the device.

Use **undo routing-table limit** to restore the default.

Syntax

routing-table limit *number* **simply-alert**

undo routing-table limit

Default

The maximum number of active IPv4/IPv6 routes is not set for the device.

Views

RIB IPv4 address family view

RIB IPv6 address family view

Predefined user roles

network-admin

Parameters

number: Specifies the maximum number of active IPv4/IPv6 routes supported by the device, in the range of 1 to 4294967295.

simply-alert: Enables the device to still accept active routes but generate a log message when the number of active IPv4/IPv6 routes exceeds the maximum number.

Usage guidelines

Configuration in RIB IPv4 address family view limits the number of active IPv4 routes.

Configuration in RIB IPv6 address family view limits the number of active IPv6 routes.

Examples

In RIB IPv4 address family view, set the maximum number of active IPv4 routes to 1000. The device still accepts new active routes but generates a system log message when the maximum number of active routes is exceeded.

```
<Sysname> system-view
[Sysname] rib
[Sysname-rib] address-family ipv4
[Sysname-rib-ipv4] routing-table limit 1000 simply-alert
```

Contents

Static routing commands

delete static-routes all

Use **delete static-routes all** to delete all static routes.

Syntax

delete static-routes all

Views

System view

Predefined user roles

network-admin

Usage guidelines

CAUTION:

This command might interrupt network communication and cause packet forwarding failure. Before executing the command, make sure you fully understand the potential impact on the network.

When you use this command, the system will prompt you to confirm the operation before deleting all the static routes.

To delete one static route, use the **undo ip route-static** command. To delete all static routes, including the default route, use the **delete static-routes all** command.

Examples

Delete all static routes.

```
<Sysname> system-view
[Sysname] delete static-routes all
This will erase all IPv4 static routes and their configurations, you must reconfigure all static routes.
Are you sure?[Y/N]:y
```

Related commands

ip route-static

display route-static nib

Use **display route-static nib** to display static route next hop information.

Syntax

display route-static nib [*nib-id*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

nib-id: Specifies a NIB by its ID, a hexadecimal string of 1 to ffffffff. If you do not specify this argument, the command displays all static route next hop information.

verbose: Displays detailed static route next hop information. If you do not specify this keyword, the command displays brief static route next hop information.

Examples

Displays brief static route next hop information.

```
<Sysname> display route-static nib
Total number of nexthop(s): 44

     NibID: 0x11000000       Sequence: 0
      Type: 0x21             Flushed: Yes
  UserKey0: 0x111             VrfNthp: 0
  UserKey1: 0x0               Nexthop: 0.0.0.0
   IFIndex: 0x111           LocalAddr: 0.0.0.0
  TopoNthp: 0                 ExtType: 0x0

     NibID: 0x11000001       Sequence: 1
      Type: 0x41             Flushed: Yes
  UserKey0: 0x0               VrfNthp: 5
  UserKey1: 0x0               Nexthop: 2.2.2.2
   IFIndex: 0x0             LocalAddr: 0.0.0.0
  TopoNthp: 0                 ExtType: 0x0

...
```

Table 1 Command output

Field	Description
NibID	ID of the NIB.
NibSeq	Sequence number of the NIB.
Type	Type of the NIB.
Flushed	Indicates whether the route with the NIB has been flushed to the FIB.
UserKey0	Reserved data 1.
UserKey1	Reserved data 2.
VrfNthp	This field is not supported in the current software version. Index of the VPN instance that the next hop belongs to. This field displays **0** if the next hop is on the IPv4 public network.
Nexthop	Next hop address.
IFIndex	Interface index
LocalAddr	Local interface address.
TopoNthp	This field is not supported in the current software version. Index of the topology that contains the next hop. This field displays **0** if the next hop is on the IPv4 public network.
ExtType	NIB extension type.

Displays detailed static route next hop information.

```
<Sysname> display route-static nib verbose
Total number of nexthop(s): 44

     NibID: 0x11000000       Sequence: 0
      Type: 0x21             Flushed: Yes
   UserKey0: 0x111            VrfNthp: 0
   UserKey1: 0x0              Nexthop: 0.0.0.0
    IFIndex: 0x111          LocalAddr: 0.0.0.0
   TopoNthp: 0                ExtType: 0x0
     RefCnt: 2            FlushRefCnt: 0
       Flag: 0x2              Version: 1
 1 nexthop(s):
PrefixIndex: 0            OrigNexthop: 0.0.0.0
  RelyDepth: 0            RealNexthop: 0.0.0.0
  Interface: NULL0          LocalAddr: 0.0.0.0
  TunnelCnt: 0                  Vrf: default-vrf
   TunnelID: N/A              Topology: base
     Weight: 1000000

     NibID: 0x11000001       Sequence: 1
      Type: 0x41             Flushed: Yes
   UserKey0: 0x0              VrfNthp: 5
   UserKey1: 0x0              Nexthop: 2.2.2.2
    IFIndex: 0x0            LocalAddr: 0.0.0.0
   TopoNthp: 0                ExtType: 0x0
     RefCnt: 1            FlushRefCnt: 0
       Flag: 0x12             Version: 1
 2 nexthop(s):
PrefixIndex: 0            OrigNexthop: 2.2.2.2
  RelyDepth: 7            RealNexthop: 8.8.8.8
  Interface: Vlan11         LocalAddr: 12.12.12.12
  TunnelCnt: 0                  Vrf: default-vrf
   TunnelID: N/A              Topology: base
     Weight: 1000000
PrefixIndex: 0            OrigNexthop: 2.2.2.2
  RelyDepth: 9            RealNexthop: 0.0.0.0
  Interface: NULL0          LocalAddr: 0.0.0.0
  TunnelCnt: 0                  Vrf: default-vrf
   TunnelID: N/A              Topology: base
     Weight: 1000000

...
```

Table 2 Command output

Field	Description
x nexthop(s)	Number of next hops.
PrefixIndex	Prefix index of the next hop for an ECMP route.

Field	Description
OrigNexthop	Original next hop.
RelyDepth	Recursion depth.
RealNexthop	Real next hop.
Interface	Output interface.
localAddr	Local interface address.
TunnelCnt	This field is not supported in the current software version. Number of tunnels after route recursion.
Vrf	This field is not supported in the current software version. VPN instance name. For the IPv4 public network, this field displays **default-vrf**.
TunnelID	This field is not supported in the current software version. ID of the tunnel after route recursion.
Topology	This field is not supported in the current software version. Topology name. The topology name for the IPv4 public network is **base**.
Weight	ECMP routes are not supported in the current software version. ECMP route weight. This field displays 0 for non-ECMP routes.
RefCnt	Reference count of the next hop.
FlushRefCnt	Reference count of the next hop that is flushed to the FIB.
Flag	Flag of the next hop.
Version	Version of the next hop.
ExtType	NIB extension type.

display route-static routing-table

Use **display route-static routing-table** to display static routing table information.

Syntax

display route-static routing-table [*ip-address* { *mask-length* | *mask* }]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ip-address: Specifies the destination IP address in dotted decimal notation. If you do not specify this argument, the command displays all static routing table information.

mask-length: Specifies the mask length, an integer in the range of 0 to 32.

mask: Specifies the subnet mask in dotted decimal notation.

Examples

Display static routing table information.

```
<Sysname> display route-static routing-table
Total number of routes: 24

Status: * - valid

*Destination: 0.0.0.0/0
      NibID: 0x1100000a       NextHop: 2.2.2.10
   MainNibID: N/A           BkNextHop: N/A
     BkNibID: N/A           Interface: Vlan-interface11
     TableID: 0x2         BkInterface: Vlan-interface12
        Flag: 0x82d01        BfdSrcIp: N/A
     DbIndex: 0xd          BfdIfIndex: 0x0
        Type: Normal       BfdVrfIndex: 0
  TrackIndex: 0xffffffff        Label: NULL
  Preference: 60          vrfIndexDst: 0
     BfdMode: N/A          vrfIndexNH: 0
   Permanent: 0                  Tag: 0

 Destination: 0.0.0.0/0
      NibID: 0x1100000b       NextHop: 2.2.2.11
   MainNibID: N/A           BkNextHop: N/A
     BkNibID: N/A           Interface: Vlan-interface13
     TableID: 0x2         BkInterface: Vlan-interface14
        Flag: 0x82d01        BfdSrcIp: N/A
     DbIndex: 0xd          BfdIfIndex: 0x0
        Type: Normal       BfdVrfIndex: 0
  TrackIndex: 0xffffffff        Label: NULL
  Preference: 60          vrfIndexDst: 0
     BfdMode: N/A          vrfIndexNH: 0
   Permanent: 0                  Tag: 0

...
```

Table 3 Command output

Field	Description
destination	Destination address/prefix.
NibID	ID of the NIB.
MainNibID	ID of the primary next hop for static route FRR.
BkNibID	ID of the backup next hop for static route FRR.
NextHop	Next hop address.
BkNextHop	Backup next hop address.
Interface	Output interface of the route.
BkInterface	Backup output interface.
TableID	ID of the table to which the route belongs.

Field	Description
Flag	Flag of the route.
DbIndex	Index of the database to which the route belongs.
Type	Route type: • Normal. • DHCP. • NAT. • IPsec.
BfdSrcIp	Source IP address of the indirect BFD session.
BfdIfIndex	Index of the interface where BFD is enabled.
BfdVrfIndex	This field is not supported in the current software version. Index of the VPN instance where BFD is enabled. This field displays **0** if BFD is enabled for the IPv4 public network.
BfdMode	BFD session mode: • **N/A**—No BFD session is configured. • **Ctrl**—Control packet mode • **Echo**—Echo packet mode.
TrackIndex	NQA Track index.
vrfIndexDst	This field is not supported in the current software version. Index of VPN instance that the destination belongs to. For the IPv4 public network, this field displays **0**.
vrfIndexNH	This field is not supported in the current software version. Index of the VPN instance that the next hop belongs to. For the IPv4 public network, this field displays **0**.
Permanent	Permanent static route flag. 1 indicates a permanent static route.

ip route-static

Use **ip route-static** to configure a static route.

Use **undo ip route-static** to delete a static route.

Syntax

ip route-static { *dest-address* { *mask-length* | *mask* } | **group** *group-name* } { *interface-type interface-number* [*next-hop-address* [**nexthop-index** *index-string*]] [**backup-interface** *interface-type interface-number* [**backup-nexthop** *backup-nexthop-address*] [**permanent**] | **bfd** { **control-packet** | **echo-packet** } | **permanent** | **track** *track-entry-number*] | *next-hop-address* [**nexthop-index** *index-string*] [**recursive-lookup host-route**] [**bfd control-packet bfd-source** *ip-address* | **permanent** | **track** *track-entry-number*] } [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]

undo ip route-static { *dest-address* { *mask-length* | *mask* } | **group** *group-name* } [*interface-type interface-number* [*next-hop-address*] | *next-hop-address*] [**preference** *preference*]

Default

No static route is configured.

Views

System view

Predefined user roles

network-admin

Parameters

dest-address: Specifies the destination IP address of the static route, in dotted decimal notation.

mask-length: Specifies the mask length, an integer in the range of 0 to 32.

mask: Specifies the subnet mask in dotted decimal notation.

group *group-name*: Specifies a static route group by its name, a case-sensitive string of 1 to 31 characters.

interface-type interface-number: Specifies an output interface by its type and number. For more information, see *Layer 3—IP Routing Configuration Guide*.

next-hop-address: Specifies the IP address of the next hop, in dotted decimal notation. For more information, see *Layer 3—IP Routing Configuration Guide*.

nexthop-index *index-string*: Specifies the index of the next hop. The *index-string* argument represents the index, which is a case-insensitive string of 1 to 93 characters. If you do not specify an index for the next hop, the static route uses the output interface and the IP address of the next hop as the next hop index. Do not specify the same next hop index for routes to the same destination.

recursive-lookup host-route: Specifies only host routes for static route recursion.

backup-interface *interface-type interface-number*: Specifies a backup output interface by its type and number. If the backup output interface is an NBMA interface or broadcast interface and not a P2P interface, you must specify the backup next hop address.

backup-nexthop *backup-nexthop-address*: Specifies a backup next hop address.

bfd: Enables BFD to detect reachability of the static route's next hop. When the next hop is unreachable, the system immediately switches to the backup route.

control-packet: Specifies the BFD control packet mode.

bfd-source *ip-address*: Specifies the source IP address of BFD packets. As a best practice, specify the loopback interface address.

echo-packet: Specifies the BFD echo packet mode.

permanent: Specifies the route as a permanent static route. If the output interface is down, the permanent static route is still active.

track *track-entry-number*: Associates the static route with a track entry specified by its number in the range of 1 to 1024. For more information about Track, see *High Availability Configuration Guide*.

preference *preference*: Specifies a preference for the static route, in the range of 1 to 255. The default is 60.

tag *tag-value*: Sets a tag value for marking the static route, in the range of 1 to 4294967295. The default is 0. Tags of routes are used for route control in routing policies. For more information about routing policies, see *Layer 3—IP Routing Configuration Guide*.

description *text*: Configures a description of 1 to 60 characters for the static route. The description can include special characters, such as the space, except the question mark (?).

Usage guidelines

If the destination IP address and the mask are both 0.0.0.0 (or 0), the configured route is a default route. The default route is used for forwarding a packet matching no entry in the routing table.

Implement different routing policies to configure different route preferences. For example, to enable backup for multiple routes to the same destination, assign different preferences to the routes.

Follow these guidelines when you specify the output interface or the next hop address of the static route:

- If the output interface is a Null 0 interface, no next hop address is required.
- If the output interface is a point-to-point interface, you can specify only the output interface. You do not need to change the configuration of the route even if the peer address is changed.
- NBMA or P2MP interfaces need IP address-to-link layer address mappings for successful packet delivery. As a best practice, specify the next hop address for the route at the same time if the output interface is an NBMA or P2MP interface.
- If the output interface is a broadcast interface, the device uses the next hop IP address to obtain the MAC address of the next hop. Therefore, you must specify both the output interface and next hop IP address, except for certain cases.

Follow these guidelines when you configure a static route:

- Enabling BFD for a flapping route could worsen the route flapping situation. Therefore, use it with caution. For more information about BFD, see *High Availability Configuration Guide*.
- If a static route needs route recursion, the associated track entry must monitor the next hop of the related route instead of that of the recursive static route. Otherwise, a valid route might be mistakenly considered invalid.
- Do not specify the **permanent** keyword together with the **bfd** or **track** keyword.

To specify the **recursive-lookup host-route** keyword, you must enable ARP direct route advertisement to advertise 32-bit host routes on the output interface corresponding to the next hop. To enable ARP direct route advertisement, use the **arp route-direct advertise** command.

If you specify a static route group, all prefixes in the static route group will be assigned the next hop and output interface specified by using this command.

Examples

Configure a static route, whose destination address is 1.1.1.1/24, next hop address is 2.2.2.2, tag value is 45, and description information is **for internet**.

```
<Sysname> system-view
[Sysname] ip route-static 1.1.1.1 24 2.2.2.2 tag 45 description for internet
```

Related commands

arp route-direct advertise (*Layer 3—IP Services Command Reference*)

display ip routing-table protocol

ip route-static-group

prefix

ip route-static arp-request

Use **ip route-static arp-request** to enable periodic sending of ARP requests to the next hops of static routes.

Use **undo ip route-static arp-request** to disable periodic sending of ARP requests to the next hops of static routes.

Syntax

ip route-static arp-request [**interval** *interval*]

undo ip route-static arp-request

Default

Periodic sending of ARP requests to the next hops of static routes is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies an ARP request sending interval in the range of 1 to 300 seconds. The default value is 5.

Usage guidelines

When the following conditions exist, a recursive static route becomes inactive:

- The static route uses a host route to reach its direct next hop.
- The host route is obtained either by specifying the **recursive-lookup host-route** keyword in the **ip route-static** command or by routing policy-based recursive lookup.
- The host route is unavailable because the direct next hop cannot send gratuitous ARP messages and consequently no ARP entry exists for that host route on the device.

To resolve this issue, you can use this command to enable the device to periodically send ARP requests to the direct next hop. When the device receives an ARP response from the direct next hop, it stops sending ARP requests and activates the recursive static route.

This command applies only to a recursive static route that meets the following requirements:

- The static route has no output interface specified.
- The static route fails the next-hop recursion.

Examples

Enable sending of ARP requests to the next hops of static routes and set the sending interval to 10 seconds.

```
<Sysname> system-view
[Sysname] ip route-static arp-request interval 10
```

Related commands

ip route-static

protocol nexthop recursive-lookup

ip route-static default-preference

Use **ip route-static default-preference** to configure a default preference for static routes.

Use **undo ip route-static default-preference** to restore the default.

Syntax

ip route-static default-preference *default-preference*

undo ip route-static default-preference

Default

The default preference of static routes is 60.

Views

System view

Predefined user roles

network-admin

Parameters

default-preference: Specifies a default preference for static routes, in the range of 1 to 255.

Usage guidelines

If no preference is specified for a static route, the default preference applies.

When the default preference is reconfigured, it applies only to newly added static routes.

Examples

Set a default preference of 120 for static routes.

```
<Sysname> system-view
[Sysname] ip route-static default-preference 120
```

Related commands

display ip routing-table protocol

ip route-static fast-reroute auto

Use **ip route-static fast-reroute auto** to configure static route FRR to automatically select a backup next hop.

Use **undo ip route-static fast-reroute auto** to disable static route FRR from automatically selecting a backup next hop.

Syntax

ip route-static fast-reroute auto

undo ip route-static fast-reroute auto

Default

Static route FRR is disabled from automatically selecting a backup next hop.

Views

System view

Predefined user roles

network-admin

Examples

Configure static route FRR to automatically select a backup next hop.

```
<Sysname> system-view
[Sysname] ip route-static fast-reroute auto
```

ip route-static primary-path-detect bfd echo

Use **ip route-static primary-path-detect bfd echo** to enable BFD echo packet mode for static route FRR.

Use **undo ip route-static primary-path-detect bfd** to disable BFD echo packet mode for static route FRR.

Syntax

ip route-static primary-path-detect bfd echo

undo ip route-static primary-path-detect bfd

Default

BFD echo packet mode for static route FRR is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command enables static route FRR to use BFD echo packet mode for fast failure detection on the primary link.

Examples

Enable BFD echo packet mode for static route FRR.

```
<Sysname> system-view
[Sysname] ip route-static 1.1.1.1 32 vlan-interface 10 2.2.2.2 backup-interface
vlan-interface 11 backup-nexthop 3.3.3.3
[Sysname] ip route-static primary-path-detect bfd echo
```

ip route-static-group

Use **ip route-static-group** to create a static route group and enter its view, or enter the view of an existing static route group.

Use **undo ip route-static-group** to delete a static route group.

Syntax

ip route-static-group *group-name*

undo ip route-static-group *group-name*

Default

No static route groups exist.

Views

System view

Predefined user roles

network-admin

Parameters

group-name: Specifies the static route group name, a case-sensitive string of 1 to 31 characters.

Examples

Create static route group **test** and enter its view.

```
<Sysname> system-view
[Sysname] ip route-static-group test
[Sysname-route-static-group-test]
```

Related commands

ip route-static

prefix

prefix

Use **prefix** to add a static route prefix to a static route group.

Use **undo prefix** to delete a static route prefix from a static route group.

Syntax

prefix *dest-address* { *mask-length* | *mask* }

undo prefix *dest-address* { *mask-length* | *mask* }

Default

No static route prefix is added to a static route group.

Views

Static route group view

Predefined user roles

network-admin

Parameters

dest-address: Specifies the destination IP address of the static route, in dotted decimal notation.

mask-length: Specifies the mask length, an integer in the range of 0 to 32.

mask: Specifies the subnet mask in dotted decimal notation.

Usage guidelines

Execute this command repeatedly to add multiple static route prefixes to a static route group.

After you add static route prefixes to a static route group, you can specify that group in the **ip route-static group** command to configure static routes with the prefixes. To configure more static routes, you only need to add new static route prefixes to the group.

Examples

Add static route prefix 1.1.1.1/32 to static route group **test**.

```
<Sysname> system-view
[Sysname] ip route-static-group test
[Sysname-route-static-group-test] prefix 1.1.1.1 32
```

Related commands

ip route-static

ip route-static-group

Contents

RIP commands

The S5000V3-EI, S5000V5-EI, S5000E-X, S5000X-EI, and WAS6000 switch series do not support RIP.

checkzero

Use **checkzero** to enable zero field check on RIPv1 messages.

Use **undo checkzero** to disable zero field check.

Syntax

checkzero

undo checkzero

Default

The zero field check function is enabled.

Views

RIP view

Predefined user roles

network-admin

Usage guidelines

When the zero field check is enabled, the router discards RIPv1 messages in which zero fields contain non-zero values. If all messages are trustworthy, disable this feature to reduce the workload of the CPU.

Examples

Disable zero field check on RIPv1 messages for RIP process 1.

```
<Sysname> system-view
[Sysname] rip
[Sysname-rip-1] undo checkzero
```

default cost

Use **default cost** to configure a default metric for redistributed routes.

Use **undo default cost** to restore the default.

Syntax

default cost *cost-value*

undo default cost

Default

The default metric of redistributed routes is 0.

Views

RIP view

Predefined user roles

network-admin

Parameters

cost-value: Specifies a default metric for redistributed routes, in the range of 0 to 16.

Usage guidelines

When you use the **import-route** command to redistribute routes from another routing protocol without specifying a metric, the metric specified by the **default cost** command applies.

Examples

Configure a default metric of 3 for redistributed routes.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] default cost 3
```

Related commands

import-route

default-route

Use **default-route** to configure all interfaces running a RIP process to advertise a default route with a specified metric to RIP neighbors.

Use **undo default-route** to restore the default.

Syntax

default-route { **only** | **originate** } [**cost** *cost-value* | **route-policy** *route-policy-name*]*

undo default-route

Default

No default route is sent to RIP neighbors.

Views

RIP view

Predefined user roles

network-admin

Parameters

only: Advertises only a default route.

originate: Advertises both a default route and other routes.

cost-value: Specifies a cost for the default route, in the range of 1 to 15. The default is 1.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case sensitive string of 1 to 63 characters. If you specify this option, the command advertises a default route only when a route in the routing table matches the routing policy.

Usage guidelines

A RIP router configured with this feature does not receive any default route from RIP neighbors.

Examples

Configure all interfaces running RIP process 100 to send only a default route with a metric of 2 to RIP neighbors.

```
<Sysname> system-view
[Sysname] rip 100
```

```
[Sysname-rip-100] default-route only cost 2
```

Related commands

rip default-route

display rip

Use **display rip** to display state and configuration information for a RIP process.

Syntax

display rip [*process-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535. If no process is specified, the command displays state and configuration information for all RIP processes.

Examples

Display current state and configuration information for all RIP processes.

```
<Sysname> display rip
  Public VPN-instance name:
    RIP process: 1
       RIP version: 1
       Preference: 100
           Routing policy: abc
       Fast-reroute:
           Routing policy: frr
       Checkzero: Enabled
       Default cost: 0
       Summary: Enabled
       Host routes: Enabled
       Maximum number of load balanced routes: 1
       Update time   :   30 secs  Timeout time         :  180 secs
       Suppress time :  120 secs  Garbage-collect time :  120 secs
       Update output delay:   20(ms)  Output count:    3
       Graceful-restart interval:   60 secs
       Triggered Interval : 5 50 200
       Silent interfaces: None
       Default routes: Originate  Default routes cost: 3
       Verify-source: Enabled
       Networks:
           1.0.0.0
       Configured peers:
           197.168.6.2
       Triggered updates sent: 0
```

```
Number of routes changes: 1
Number of replies to queries: 0
```

Table 1 Command output

Field	Description
Public VPN-instance name	The RIP process runs on the public network.
RIP process	RIP process ID.
RIP version	RIP version 1 or 2.
Preference	RIP preference.
Checkzero	Indicates whether the zero field check is enabled for RIPv1 messages: **Enabled** or **Disabled**.
Default cost	Default cost of redistributed routes.
Summary	Indicates whether route summarization is enabled: **Enabled** or **Disabled**.
Host routes	Indicates whether to receive host routes: **Enabled** or **Disabled**.
Maximum number of load balanced routes	ECMP routes are not supported in the current software version. Maximum number of load-balanced routes.
Update time	RIP update interval, in seconds.
Timeout time	RIP timeout time, in seconds.
Suppress time	RIP suppress interval, in seconds.
Garbage-collect time	RIP garbage-collect interval, in seconds.
Update output delay	RIP packet sending interval, in seconds.
Output count	Maximum number of RIP packets sent at each interval.
Graceful-restart interval	GR interval, in seconds.
Triggered Interval	Triggered update sending interval.
Silent interfaces	Silent interfaces, which do not periodically send updates.
Default routes	Indicates whether a default route is sent to RIP neighbors. • **only**—Only a default route is advertised. • **originate**—A default route is advertised along with other routes. • **disable**—No default route is advertised.
Default routes cost	Metric for a default route.
Verify-source	Indicates whether the source IP address is checked for received RIP routing updates: **Enabled** or **Disabled**.
Networks	Networks enabled with RIP.
Configured peers	Configured neighbors.
Triggered updates sent	Number of triggered updates sent.
Number of routes changes	Number of route changes.

Field	Description
Number of replies to queries	Number of RIP responses.

display rip database

Use **display rip database** to display active routes for a RIP process.

Syntax

display rip *process-id* **database** [*ip-address* { *mask-length* | *mask* }]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535.

ip-address { *mask-length* | *mask* }: Displays active routes for the specified IP address. If you do not specify this argument, the command displays all actives routes for a RIP process.

Examples

Display active routes for RIP process 100.

```
<Sysname> display rip 100 database
   1.0.0.0/8, auto-summary
       1.1.1.0/24, cost 16, interface summary
       1.1.1.0/24, cost 0, nexthop 1.1.1.1, RIP-interface
       1.1.2.0/24, cost 0, imported
   2.0.0.0/8, auto-summary
   2.0.0.0/8, cost 1, nexthop 1.1.1.2
```

Display active routes with destination IP address 1.1.1.0 and mask length 24 for RIP process 100.

```
<Sysname> display rip 100 database 1.1.1.0 24
   1.1.1.0/24, cost 16, interface summary
   1.1.1.0/24, cost 0, nexthop 1.1.1.1, RIP-interface
```

Table 2 Command output

Field	Description
cost	Cost of the route.
auto-summary	Indicates that the route is a RIP automatic summary route.
interface summary	Indicates that the route is a RIP interface summary route.
nexthop	Address of the next hop.
RIP-interface	Direct route on a RIP-enabled interface.
imported	Indicates that the route is redistributed from another routing protocol.

display rip graceful-restart

Use **display rip graceful-restart** to display the GR status for a RIP process.

Syntax

display rip [*process-id*] **graceful-restart**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays the GR status for all RIP processes.

Examples

Display the GR status for RIP process 1.

```
<Sysname> display rip 1 graceful-restart
 RIP process: 1
 Graceful Restart capability     : Enabled
 Current GR state                : Normal
 Graceful Restart period         : 60  seconds
 Graceful Restart remaining time : 0   seconds
```

Table 3 Command output

Field	Description
Graceful Restart capability	Indicates whether GR is enabled: **Enabled** or **Disabled**.
Current GR state	GR state: • **Under GR**—GR is in progress. • **Normal**—No GR is in progress or GR has completed.
Graceful Restart period	GR interval.

display rip interface

Use **display rip interface** to display RIP interface information for a RIP process.

Syntax

display rip *process-id* **interface** [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535.

interface-type interface-number: Specifies an interface by its type and number. If no interface is specified, the command displays information about all RIP interfaces for the RIP process.

Examples

Display information about all interfaces for RIP process 1.

```
<Sysname> display rip 1 interface
Total: 1

 Interface: Vlan-interface10
    Address/Mask: 1.1.1.1/24          Version: RIPv1
    MetricIn: 0                       MetricIn route policy: Not designated
    MetricOut: 1                      MetricOut route policy: Not designated
    Split-horizon/Poison-reverse: On/Off  Input/Output: On/On
    Default route: Off
    Update output delay:  20(ms)      Output count: 3
    Current number of packets/Maximum number of packets: 0/2000
```

Table 4 Command output

Field	Description
Total	Number of interfaces running RIP.
Interface	Name of an interface running RIP.
Address/Mask	IP address and mask of the interface.
Version	RIP version running on the interface.
MetricIn	Additional metric added to incoming routes.
MetricIn route policy	Name of the routing policy used to add an additional metric for incoming routes. If no routing policy is used, the field displays **Not designated**.
MetricOut	Additional metric added to outgoing routes.
MetricOut route policy	Name of the routing policy used to add an additional routing metric for outgoing routes. If no routing policy is used, the field displays **Not designated**.
Split-horizon	Indicates whether split horizon is enabled: • **on**—Enabled. • **off**—Disabled.
Poison-reverse	Indicates whether poison reverse is enabled: • **on**—Enabled. • **off**—Disabled.
Input/Output	Indicates whether the interface is enabled to receive and send RIP messages: • **on**—Enabled. • **off**—Disabled.
Default route	Indicates whether to send a default route to RIP neighbors: • **Only**—Advertises only a default route. • **Originate**—Advertises both a default route and other routes. • **No-originate**—Advertises only non-default routes.

Field	Description
	• **Off**—Advertises no default route.
Default route cost	Metric for a default route.
Update output delay	RIP packet sending interval.
Output count	Maximum number of RIP packets that can be sent at each interval.
Current number of packets /Maximum number of packets	Number of RIP packets to be sent/maximum number of RIP packets that can be sent within a certain interval.

display rip neighbor

Use **display rip neighbor** to display neighbor information for a RIP process.

Syntax

display rip *process-id* **neighbor** [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify this argument, the command displays all neighbor information for the RIP process.

Examples

Display neighbor information for RIP process 1.

```
<Sysname> display rip 1 neighbor
 Neighbor address: 197.168.2.3
     Interface  : Vlan-interface10
     Version    : RIPv2     Last update: 00h00m02s
     Relay nbr  : N/A       BFD session: N/A
     Bad packets: 0         Bad routes : 0
```

Table 5 Command output

Field	Description
Interface	Output interface that is connected to the neighbor.
Version	Version of RIP that the neighbor runs.
Last update	Time elapsed since the most recent update.
Relay nbr	Relay neighbor type.
BFD session	BFD session type.
Bad packets	Number of received bad packets.
Bad routes	Number of received bad routes.

display rip non-stop-routing

Use **display rip non-stop-routing** to display the NSR status for a RIP process.

Syntax

display rip [*process-id*] **non-stop-routing**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays the NSR status for all RIP processes.

Examples

Display the NSR status for RIP process 1.

```
<Sysname> display rip 1 non-stop-routing
RIP process: 1
 Nonstop Routing capability: Enabled
 Current NSR state         : Finish
```

Table 6 Command output

Field	Description
Nonstop Routing capability	Indicates whether NSR is enabled: **Enabled** or **Disabled**.
Current NSR state	NSR state: • Initialization. • **Smooth**—Upgrading data. • **Advertising**—Advertising routes. • **Redistribution**—Redistributing routes. • Finish.

display rip route

Use **display rip route** to display routing information for a RIP process.

Syntax

display rip *process-id* **route** [*ip-address* { *mask-length* | *mask* } [**verbose**] | **peer** *ip-address* | **statistics**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535.

ip-address { *mask-length* | *mask* }: Displays route information for the specified IP address.

verbose: Displays all routing information for the specified destination IP address. If you do not specify this keyword, the command displays only information about optimal routes with the specified destination IP address.

peer *ip-address*: Displays route information learned from the specified neighbor.

statistics: Displays route statistics, including the total number of routes and number of routes from each neighbor.

Usage guidelines

If no optional parameters are specified, the **display rip** *process-id* **route** command displays all routing information for a RIP process.

Examples

Display all routing information for RIP process 1.

```
<Sysname> display rip 1 route
 Route Flags: R - RIP, T - TRIP
              P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
              D - Direct, O - Optimal, F - Flush to RIB
------------------------------------------------------------------------------
 Peer 1.1.1.1 on Vlan-interface10
      Destination/Mask        Nexthop          Cost    Tag     Flags   Sec
      3.0.0.0/8               1.1.1.1          1       0       RAOF    24
 Local route
      Destination/Mask        Nexthop          Cost    Tag     Flags   Sec
      4.4.4.4/32              0.0.0.0          0       0       RDOF    -
      1.1.1.0/24              0.0.0.0          0       0       RDOF    -
```

Display specified routing information for RIP process 1.

```
<Sysname> display rip 1 route 3.0.0.0 8 verbose
 Route Flags: R - RIP, T - TRIP
              P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
              D - Direct, O - Optimal, F - Flush to RIB
------------------------------------------------------------------------------
 Peer 1.1.1.1 on Vlan-interface10
  Destination/Mask    OrigNexthop/RealNexthop          Cost  Tag   Flags Sec
  3.0.0.0/8           1.1.1.1/1.1.1.1                  1     0     RAOF  16
```

Table 7 Command output

Field	Description
Route Flags	• **R**—RIP route. • **P**—The route never ages out. • **A**—The route is aging. • **S**—The route is suppressed. • **G**—The route is in Garbage-collect state. • **D**—The route is a direct route. • **O**—The route is an optimal route. • **F**—The route has been flushed to the RIB.

Field	Description
Peer *X.X.X.X* on *interface-type interface-number*	Routing information learned from a neighbor on a RIP interface.
Local route	Locally generated direct routes.
Destination/Mask	Destination IP address and subnet mask.
Nexthop	Next hop of the route.
OrigNexthop/RealNexthop	If the route is from a directly connected neighbor, the original next hop is the real next hop. If the route is from an indirectly connected neighbor, the **RealNexthop** field displays the recursive next hop for the route. Otherwise, the field is blank.
Cost	Cost of the route.
Tag	Route tag.
Flags	Route state.
Sec	Remaining time of the timer corresponding to the route state.

Display routing statistics for RIP process 1.

```
<Sysname> display rip 1 route statistics
 Peer                    Optimal/Aging       Optimal/Permanent       Garbage
 1.1.1.1                 1/1                 0/0                     0
 Local                   2/0                 0/0                     0
 Total                   3/1                 0/0                     0
```

Table 8 Command output

Field	Description
Peer	IP address of a neighbor.
Optimal	Total number of optimal routes.
Aging	Total number of aging routes.
Permanent	Total number of routes that never age out.
Garbage	Total number of routes in the Garbage-collection state.
Local	Total number of locally generated direct routes.
Total	Total number of routes learned from all RIP neighbors.

dscp

Use **dscp** to set the DSCP value for outgoing RIP packets.

Use **undo dscp** to restore the default.

Syntax

dscp *dscp-value*

undo dscp

Default

The DSCP value for outgoing RIP packets is 48.

Views

RIP view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies the DSCP value in the range of 0 to 63.

Examples

Set the DSCP value for outgoing RIP packets to 63 in RIP process 1.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] dscp 63
```

fast-reroute

Use **fast-reroute** to configure RIP FRR.

Use **undo fast-reroute** to disable RIP FRR.

Syntax

fast-reroute route-policy *route-policy-name*

undo fast-reroute

Default

RIP FRR is disabled.

Views

RIP view

Predefined user roles

network-admin

Parameters

route-policy *route-policy-name*: Specifies a routing policy by its name, a case sensitive string of 1 to 63 characters. If you specify this option, the command designates a backup next hop for the routes that match the routing policy.

Usage guidelines

RIP FRR is available only when the state of primary link (with Layer 3 interfaces staying up) changes from bidirectional to unidirectional or down. A unidirectional link refers to the link through which packets are forwarded only from one end to the other.

RIP FRR is only effective for RIP routes that are learned from directly connected neighbors.

Examples

Enable RIP FRR and use routing policy **frr** to specify a backup next hop.

```
<Sysname> system-view
[Sysname] ip prefix-list abc index 10 permit 100.1.1.0 24
[Sysname] route-policy frr permit node 10
[Sysname-route-policy-frr-10] if-match ip address prefix-list abc
[Sysname-route-policy-frr-10] apply fast-reroute backup-interface vlan-interface 1
backup-nexthop 193.1.1.8
[Sysname-route-policy-frr-10] quit
```

```
[Sysname] rip 100
[Sysname-rip-100] fast-reroute route-policy frr
```

filter-policy export

Use **filter-policy export** to configure RIP to filter redistributed routes.

Use **undo filter-policy export** to remove the filtering.

Syntax

filter-policy { *ipv4-acl-number* | **prefix-list** *prefix-list-name* } **export** [*protocol* [*process-id*] | *interface-type interface-number*]

undo filter-policy export [*protocol* [*process-id*] | *interface-type interface-number*]

Default

RIP does not filter redistributed routes.

Views

RIP view

Predefined user roles

network-admin

Parameters

ipv4-acl-number: Specifies an IPv4 ACL by its number in the range of 2000 to 3999 to filter redistributed routes.

prefix-list *prefix-list-name*: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter redistributed routes.

protocol: Filters routes redistributed from the specified routing protocol.

process-id: Specifies the process ID of the specified routing protocol, in the range of 1 to 65535. Specify a process ID when the routing protocol is **rip** or **ospf**. If no process ID is specified, the default process ID is 1.

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

You can configure only one filtering policy to filter routes redistributed from a routing protocol or an interface. Without any protocol or interface specified, the filtering policy applies globally. If you execute this command multiple times, the most recent configuration takes effect.

To remove the filtering policy configured for a protocol or an interface, use the **undo filter-policy export** command with the protocol or interface specified.

To reference an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL using one of the following methods:

- To deny/permit a route with the specified destination, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* command.
- To deny/permit a route with the specified destination and mask, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* **destination** *dest-addr dest-wildcard* command.

The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the subnet mask of the route. For the mask configuration to take effect, specify a contiguous subnet mask.

Examples

Use basic ACL 2000 to filter redistributed routes.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule deny source 192.168.10.0 0.0.0.255
[Sysname-acl-ipv4-basic-2000] quit
[Sysname] rip 1
[Sysname-rip-1] filter-policy 2000 export
```

Use IP prefix list **abc** to filter redistributed routes.

```
<Sysname> system-view
[Sysname] ip prefix-list abc index 10 permit 11.0.0.0 8
[Sysname] rip 1
[Sysname-rip-1] filter-policy prefix-list abc export
```

Configure advanced ACL 3000 to permit only route 113.0.0.0/16 to pass. Use ACL 3000 to filter redistributed routes.

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule 10 permit ip source 113.0.0.0 0 destination 255.255.0.0
0
[Sysname-acl-ipv4-adv-3000] rule 100 deny ip
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] rip 1
[Sysname-rip-1] filter-policy 3000 export
```

Related commands

acl (*ACL and QoS Command Reference*)

import-route

ip prefix-list

filter-policy import

Use **filter-policy import** to configure RIP to filter received routes.

Use **undo filter-policy import** to remove the filtering.

Syntax

filter-policy { *ipv4-acl-number* | **gateway** *prefix-list-name* | **prefix-list** *prefix-list-name* [**gateway** *prefix-list-name*] } **import** [*interface-type interface-number*]

undo filter-policy import [*interface-type interface-number*]

Default

RIP does not filter received routes.

Views

RIP view

Predefined user roles

network-admin

Parameters

ipv4-acl-number: Specifies an IPv4 ACL by its number in the range of 2000 to 3999 to filter received routes.

prefix-list *prefix-list-name*: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter received routes.

gateway *prefix-list-name*: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter routes based on their next hops.

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

You can configure only one filtering policy to filter routes received on an interface. Without any interface specified, the filtering policy applies globally. If you execute this command multiple times, the most recent configuration takes effect.

To remove the filtering policy configured for an interface, use the **undo filter-policy import** command with the interface specified.

To reference an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL using one of the following methods:

- To deny/permit a route with the specified destination, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* command
- To deny/permit a route with the specified destination and mask, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* **destination** *dest-addr dest-wildcard* command.

The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the subnet mask of the route. For the mask configuration to take effect, specify a contiguous subnet mask.

Examples

Use basic ACL 2000 to filter received RIP routes.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule deny source 192.168.10.0 0.0.0.255
[Sysname-acl-ipv4-basic-2000] quit
[Sysname] rip 1
[Sysname-rip-1] filter-policy 2000 import
```

Use IP prefix list **abc** to filter received RIP routes.

```
<Sysname> system-view
[Sysname] ip prefix-list abc index 10 permit 11.0.0.0 8
[Sysname] rip 1
[Sysname-rip-1] filter-policy prefix-list abc import
```

Configure advanced ACL 3000 to permit only route 113.0.0.0/16 to pass. Use ACL 3000 to filter received routes.

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule 10 permit ip source 113.0.0.0 0 destination 255.255.0.0
0
[Sysname-acl-ipv4-adv-3000] rule 100 deny ip
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] rip 1
[Sysname-rip-1] filter-policy 3000 import
```

Related commands

acl (*ACL and QoS Command Reference*)

ip prefix-list

graceful-restart

Use **graceful-restart** to enable RIP GR.

Use **undo graceful-restart** to disable RIP GR.

Syntax

graceful-restart

undo graceful-restart

Default

RIP GR is disabled.

Views

RIP view

Predefined user roles

network-admin

Usage guidelines

The **graceful-restart** command and the **non-stop-routing** command are mutually exclusive.

Examples

Enable GR for RIP process 1.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] graceful-restart
```

graceful-restart interval

Use **graceful-restart interval** to set the GR interval.

Use **undo graceful-restart interval** to restore the default.

Syntax

graceful-restart interval *interval*

undo graceful-restart interval

Default

The GR interval is 60 seconds.

Views

RIP view

Predefined user roles

network-admin

Parameters

interval: Specifies the GR interval in the range of 5 to 360 seconds.

Examples

Set the GR interval to 200 seconds for RIP process 1.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] graceful-restart interval 200
```

host-route

Use **host-route** to enable host route reception.

Use **undo host-route** to disable host route reception.

Syntax

host-route

undo host-route

Default

RIP receives host routes.

Views

RIP view

Predefined user roles

network-admin

Usage guidelines

A router might receive many host routes from the same subnet. These routes are not helpful for routing and occupy a large number of resources. To solve this problem, use the **undo host-route** command to disable RIP from receiving host routes.

This command takes effect only for RIPv2 routes.

Examples

Disable RIP from receiving host routes.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] undo host-route
```

import-route

Use **import-route** to enable route redistribution.

Use **undo import-route** to remove redistributed routes.

Syntax

import-route { **direct** | **static** } [**cost** *cost-value* | **route-policy** *route-policy-name* | **tag** *tag*] *

undo import-route { **direct** | **static** }

import-route { **ospf** | **rip** } [*process-id* | **all-processes**] [**allow-direct** | **cost** *cost-value* | **route-policy** *route-policy-name* | **tag** *tag*] *

undo import-route { **ospf** | **rip** } [*process-id* | **all-processes**]

Default

RIP does not redistribute any routes.

Views

RIP view

Predefined user roles

network-admin

Parameters

direct: Redistributes direct routes.

ospf: Redistributes OSPF routes.

rip: Redistributes RIP routes.

static: Redistributes static routes.

process-id: Specifies a process ID of OSPF or RIP, in the range of 1 to 65535. The default is 1.

all-processes: Enables route redistribution from all OSPF or RIP processes.

allow-direct: Redistributes the networks of the local interfaces enabled with the specified routing protocol. If you do not specify the **allow-direct** keyword, the networks of the local interfaces are not redistributed. If you specify both the **allow-direct** keyword and the **route-policy** *route-policy-name* option, make sure the **if-match** rule defined in the routing policy does not conflict with the **allow-direct** keyword. For example, if you specify the **allow-direct** keyword, do not configure the **if-match route-type** rule for the routing policy. Otherwise, the **allow-direct** keyword does not take effect.

cost *cost-value*: Specifies a cost for redistributed routes, in the range of 0 to 16. The default cost is 0.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

tag *tag*: Specifies a tag for marking redistributed routes, in the range of 0 to 65535. The default is 0.

Usage guidelines

This command redistributes only active routes. To view route state information, use the **display ip routing-table protocol** command.

When you execute the **undo** form of the command, per-process setting has higher priority than the all-processes setting. The **undo import-route** { **ospf** | **rip** } **all-processes** command cannot remove the setting configured for a process by using the **import-route** { **ospf** | **rip** } *process-id* command. To remove the setting for that process, you must specify the process ID in the **undo** form of the command.

Examples

Redistribute static routes into RIP, and set the cost of redistributed routes to 4.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] import-route static cost 4
```

Related commands

default cost

network

Use **network** to enable RIP on an interface attached to a specified network.

Use **undo network** to disable RIP on an interface attached to a specified network.

Syntax

network *network-address* [*wildcard-mask*]

undo network *network-address*

Default

RIP is disabled on an interface.

Views

RIP view

Predefined user roles

network-admin

Parameters

network-address: Specifies a subnet address where an interface resides.

wildcard-mask: Specifies an IP address wildcard mask. A wildcard mask can be thought of as a subnet mask, with 1s and 0s inverted. For example, a wildcard mask of 255.255.255.0 corresponds to a subnet mask of 0.0.0.255. If you do not specify this argument, the command uses the natural mask.

Usage guidelines

RIP runs only on an interface attached to the specified network, which can be configured with a wildcard mask. An interface not on the specified network does not receive or send RIP routes, or advertise its direct routes.

For a single RIP process, the **network** 0.0.0.0 command can enable RIP on all interfaces. If multiple RIP processes exist, the command is not applicable.

If a physical interface is attached to multiple networks, you cannot advertise these networks in different RIP processes.

Examples

Enable RIP process 100 on the interface attached to the network 129.102.0.0.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] network 129.102.0.0
```

Related commands

rip enable

non-stop-routing

Use **non-stop-routing** to enable RIP NSR.

Use **undo non-stop-routing** to disable RIP NSR.

Syntax

non-stop-routing

undo non-stop-routing

Default

RIP NSR is disabled.

Views

RIP view

Predefined user roles

network-admin

Usage guidelines

RIP NSR enabled for a RIP process takes effect only on that process. As a best practice, enable RIP NSR for each process if multiple RIP processes exist.

The **non-stop-routing** command and the **graceful-restart** command are mutually exclusive.

Examples

Enable NSR for RIP process 1.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] non-stop-routing
```

output-delay

Use **output-delay** to set the rate at which an interface sends RIP packets.

Use **undo output-delay** to restore the default.

Syntax

output-delay *time* **count** *count*

undo output-delay

Default

An interface sends up to three RIP packets every 20 milliseconds.

Views

RIP view

Predefined user roles

network-admin

Parameters

time: Specifies the sending interval in the range of 10 to 100 milliseconds.

count: Specifies the maximum number of RIP packets sent at each interval, in the range of 1 to 30.

Examples

Configure all interfaces running RIP process 1 to send up to 10 RIP packets every 60 milliseconds.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] output-delay 60 count 10
```

peer

Use **peer** to specify a RIP neighbor in the NBMA network, where routing updates destined for the neighbor are only unicasts and not multicast or broadcast.

Use **undo peer** to remove a RIP neighbor.

Syntax

peer *ip-address*

undo peer *ip-address*

Default

RIP does not unicast updates to any neighbor.

Views

RIP view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address of a RIP neighbor, in dotted decimal notation.

Usage guidelines

Do not use the **peer** *ip-address* command when the neighbor is directly connected. Otherwise, the neighbor might receive both unicast and multicast (or broadcast) messages with the same routing information.

This command must be executed together with the **undo validate-source-address** command, which disables source IP address check on inbound RIP routing updates.

Examples

Configure RIP to unicast updates to peer 202.38.165.1.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] peer 202.38.165.1
```

Related commands

validate-source-address

preference

Use **preference** to specify a preference for RIP routes.

Use **undo preference** to restore the default.

Syntax

preference { *preference* | **route-policy** *route-policy-name* } *

undo preference

Default

The preference of RIP routes is 100.

Views

RIP view

Predefined user roles

network-admin

Parameters

preference: Specifies a preference for RIP routes, in the range of 1 to 255. The smaller the value, the higher the preference.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

You can specify a routing policy by using the keyword **route-policy** to set a preference for matching RIP routes.

- The preference set by the routing policy applies to all matching RIP routes. The preference of other routes is set by the **preference** command.
- If no preference is set by the routing policy, the preference of all RIP routes is set by the **preference** command.

Examples

Set a preference of 120 for RIP routes.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] preference 120
```

reset rip process

Use **reset rip process** to reset a RIP process.

Syntax

reset rip *process-id* **process**

Views

User view

Predefined user roles

network-admin

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535.

Usage guidelines

After executing the command, you are prompted to confirm the operation.

Examples

Reset RIP process 100.

```
<Sysname> reset rip 100 process
Reset RIP process? [Y/N]:y
```

reset rip statistics

Use **reset rip statistics** to clear statistics for a RIP process.

Syntax

reset rip *process-id* **statistics**

Views

User view

Predefined user roles

network-admin

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535.

Examples

Clear statistics for RIP process 100.

```
<Sysname> reset rip 100 statistics
```

rip

Use **rip** to enable RIP and enter RIP view.

Use **undo rip** to disable RIP.

Syntax

rip [*process-id*]

undo rip [*process-id*]

Default

RIP is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535. The default is 1.

Usage guidelines

You must enable a RIP process before configuring global parameters for it. This restriction does not apply to configuring interface parameters.

If you disable a RIP process, the configured interface parameters become invalid.

Examples

Enable RIP process 1 and enter RIP view.

```
<Sysname> system-view
[Sysname] rip
[Sysname-rip-1]
```

rip authentication-mode

Use **rip authentication-mode** to configure RIPv2 authentication.

Use **undo rip authentication-mode** to restore the default.

Syntax

rip authentication-mode { **md5** { **rfc2082** { **cipher** | **plain** } *string key-id* | **rfc2453** { **cipher** | **plain** } *string* } | **simple** { **cipher** | **plain** } *string* }

undo rip authentication-mode

Default

RIPv2 authentication is not configured.

Views

Interface view

Predefined user roles

network-admin

Parameters

md5: Specifies the MD5 authentication.

rfc2082: Uses the message format defined in RFC 2082.

cipher: Specifies a password in encrypted form.

plain: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 16 characters. Its encrypted form is a case-sensitive string of 33 to 53 characters.

key-id: Specifies the key ID in the range of 1 to 255.

rfc2453: Uses the message format defined in RFC 2453 (IETF standard).

simple: Specifies the simple authentication mode.

Usage guidelines

A newly configured key overwrites the old one, if any.

Although you can specify an authentication mode for RIPv1 in interface view, the configuration does not take effect because RIPv1 does not support authentication.

Examples

Configure MD5 authentication on VLAN-interface 10 and specify a plaintext key **rose** in the format defined in RFC 2453.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip version 2
[Sysname-Vlan-interface10] rip authentication-mode md5 rfc2453 plain rose
```

Related commands

rip version

rip bfd enable

Use **rip bfd enable** to enable BFD for RIP on an interface.

Use **undo rip bfd enable** to restore the default.

Syntax

rip bfd enable

undo rip bfd enable

Default

BFD for RIP is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

RIP supports BFD echo-mode detection for a directly connected neighbor, and BFD control-mode detection for an indirectly neighbor.

BFD echo-mode detection only applies to a RIP neighbor one hop away.

Using the **undo peer** command does not delete the neighbor relationship immediately and cannot bring down the BFD session immediately.

The **rip bfd enable** command and the **rip bfd enable destination** command are mutually exclusive and cannot be configured on a device at the same time.

Examples

Enable BFD for RIP on VLAN-interface 11.

```
<Sysname> system-view
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] rip bfd enable
```

rip bfd enable destination

Use **rip bfd enable destination** to enable BFD single-hop echo detection for a specific destination.

Use **undo rip bfd enable** to disable BFD single-hop echo detection for RIP.

Syntax

rip bfd enable destination *ip-address*

undo rip bfd enable

Default

BFD single-hop echo detection for a specific destination is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

When a link failure occurs between the local device and the specified neighbor, BFD can detect the failure. The local device will not receive or send any RIP packets through the interface connected to the neighbor.

The **rip bfd enable destination** command applies only to BFD echo-mode detection.

The **rip bfd enable destination** command and the **rip bfd enable** command are mutually exclusive and cannot be configured on a device at the same time.

Examples

Enable BFD on VLAN-interface 10 for a specific destination 202.38.165.1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip bfd enable destination 202.38.165.1
```

rip default-route

Use **rip default-route** to configure a RIP interface to advertise a default route with a specified metric.

Use **undo rip default-route** to disable a RIP interface from sending a default route.

Syntax

rip default-route { { **only** | **originate** } [**cost** *cost-value* | **route-policy** *route-policy-name*] * | **no-originate** }

undo rip default-route

Default

A RIP interface advertises a default route if the RIP process that the interface runs is enabled to advertise a default route.

Views

Interface view

Predefined user roles

network-admin

Parameters

only: Advertises only a default route.

originate: Advertises both a default route and other routes.

cost-value: Specifies a cost for the default route, in the range of 1 to 15. The default is 1.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case sensitive string of 1 to 63 characters. If you specify this option, the command advertises a default route only when a route in the routing table matches the routing policy.

no-originate: Advertises only non-default routes.

Usage guidelines

An interface that is enabled to advertise a default route does not receive any default route from RIP neighbors.

Examples

Configure VLAN-interface 10 to advertise only a default route with a metric of 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip default-route only cost 2
```

Configure VLAN-interface 10 to advertise a default route with a metric of 2 and other routes.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip default-route originate cost 2
```

Related commands

default-route

rip enable

Use **rip enable** to enable RIP on an interface.

Use **undo rip enable** to disable RIP on an interface.

Syntax

rip *process-id* **enable** [**exclude-subip**]

undo rip enable

Default

RIP is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535.

exclude-subip: Excludes secondary IP addresses from being enabled with RIP. If you do not specify this keyword, RIP is also enabled on secondary IP addresses of a RIP-enabled interface.

Usage guidelines

The **rip enable** command has a higher priority than the **network** command.

Examples

Enable RIP process 100 on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip 100 enable
```

Related commands

network

rip input

Use **rip input** to enable an interface to receive RIP messages.

Use **undo rip input** to disable an interface from receiving RIP messages.

Syntax

rip input

undo rip input

Default

An interface is enabled to receive RIP messages.

Views

Interface view

Predefined user roles

network-admin

Examples

Disable VLAN-interface 10 from receiving RIP messages.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] undo rip input
```

rip max-packet-length

Use **rip max-packet-length** to set the maximum length of RIP packets.

Use **undo rip max-packet-length** to restore the default.

Syntax

rip max-packet-length *value*

undo rip max-packet-length

Default

The maximum length of RIP packets is 512 bytes.

Views

Interface view

Predefined user roles

network-admin

Parameters

value: Specifies the maximum length of RIP packets, in the range of 32 to 65535 bytes.

Usage guidelines

The supported maximum length of RIP packets varies by vendor. Use this feature with caution to avoid compatibility issues.

When authentication is enabled, follow these guidelines to ensure packet forwarding:

- For simple authentication, the maximum length of RIP packets must be no less than 52 bytes.
- For MD5 authentication (with packet format defined in RFC 2453), the maximum length of RIP packets must be no less than 56 bytes.
- For MD5 authentication (with packet format defined in RFC 2082), the maximum length of RIP packets must be no less than 72 bytes.

If the configured value in the **rip max-packet-length** command is greater than the MTU of an interface, the interface MTU value is used as the maximum length of RIP packets.

Examples

Set the maximum length of RIP packets on VLAN-interface 10 to 1024 bytes.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip max-packet-length 1024
```

rip metricin

Use **rip metricin** to configure an interface to add a metric to inbound routes.

Use **undo rip metricin** to restore the default.

Syntax

rip metricin [**route-policy** *route-policy-name*] *value*

undo rip metricin

Default

The additional metric of an inbound route is 0.

Views

Interface view

Predefined user roles

network-admin

Parameters

route-policy *route-policy-name*: Specifies a routing policy by its name, a case sensitive string of 1 to 63 characters. If you specify this option, the command adds an additional metric for the routes that match the routing policy.

value: Adds an additional metric to inbound routes, in the range of 0 to 16.

Usage guidelines

When a valid RIP route is received, the system adds a metric to it and then installs it into the routing table. The metric of the route received on the configured interface is then increased. If the sum of the additional metric and the original metric is greater than 16, the metric of the route will be 16.

If a routing policy is referenced with the **route-policy** keyword, the following operations can be performed:

- Routes matching the policy are added with the metric specified in the **apply cost** command configured in the policy. Routes not matching it are added with the metric specified in the **rip metricin** command. The **rip metricin** command does not support specifying the **+** or **–** keyword in the **apply cost** command to add or reduce a metric.
- If the **apply cost** command is not configured in the policy, all the inbound routes are added with the metric specified in the **rip metricin** command.

Examples

Configure VLAN-interface 10 to add a metric of 6 to the inbound route 1.0.0.0/8 and to add a metric of 2 to other inbound routes.

```
<Sysname> system-view
[Sysname] ip prefix-list 123 permit 1.0.0.0 8
[Sysname] route-policy abc permit node 10
[Sysname-route-policy-abc-10] if-match ip address prefix-list 123
[Sysname-route-policy-abc-10] apply cost 6
[Sysname-route-policy-abc-10] quit
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip metricin route-policy abc 2
```

Related commands

apply cost

rip metricout

Use **rip metricout** to configure an interface to add a metric to outbound routes.

Use **undo rip metricout** to restore the default.

Syntax

rip metricout [**route-policy** *route-policy-name*] *value*

undo rip metricout

Default

The additional metric for outbound routes is 1.

Views

Interface view

Predefined user roles

network-admin

Parameters

route-policy *route-policy-name*: Specifies a routing policy by its name, a case sensitive string of 1 to 63 characters. If you specify this option, the command adds an additional metric for the routes that match the routing policy.

value: Adds an additional metric to outbound routes, in the range of 1 to 16.

Usage guidelines

With the command configured on an interface, the metric of RIP routes sent on the interface will be increased.

If a routing policy is referenced with the **route-policy** keyword, the following operations can be performed:

- Routes matching the policy is added with the metric specified in the **apply cost** command configured in the policy. Routes not matching it are added with the metric specified in the **rip metricout** command. The **rip metricout** command does not support specifying the **+** or **–** keyword in the **apply cost** command to add or reduce a metric.
- If the **apply cost** command is not configured in the policy, all the outbound routes are added with the metric specified in the **rip metricout** command.

Examples

Configure VLAN-interface 10 to add a metric of 6 to the outbound route 1.0.0.0/8 and to add a metric of 2 to other outbound routes.

```
<Sysname> system-view
[Sysname] ip prefix-list 123 permit 1.0.0.0 8
[Sysname] route-policy abc permit node 10
[Sysname-route-policy-abc-10] if-match ip address prefix-list 123
[Sysname-route-policy-abc-10] apply cost 6
[Sysname-route-policy-abc-10] quit
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip metricout route-policy abc 2
```

Related commands

apply cost

rip mib-binding

Use **rip mib-binding** to bind a RIP process to MIB.

Use **undo rip mib-binding** to restore the default.

Syntax

rip mib-binding *process-id*

undo rip mib-binding

Default

MIB operation is bound to the RIP process with the smallest process ID.

Views

System view

Predefined user roles

network-admin

Parameters

process-id: Specifies a RIP process by its ID in the range of 1 to 65535.

Usage guidelines

If the specified process ID does not exist, the MIB binding configuration does not take effect.

Deleting a RIP process bound to MIB operation deletes the MIB binding configuration. After the RIP process is deleted, MIB operation is bound to the RIP process with the smallest process ID.

Examples

Bind RIP process 100 to MIB.

```
<Sysname> system-view
[Sysname] rip mib-binding 100
```

rip output

Use **rip output** to enable an interface to send RIP messages.

Use **undo rip output** to disable an interface from sending RIP messages.

Syntax

rip output

undo rip output

Default

An interface sends RIP messages.

Views

Interface view

Predefined user roles

network-admin

Examples

Disable VLAN-interface 10 from sending RIP messages.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] undo rip output
```

rip output-delay

Use **rip output-delay** to set the RIP packet sending interval for an interface and the maximum number of RIP packets that can be sent at each interval.

Use **undo rip output-delay** to restore the default.

Syntax

rip output-delay *time* **count** *count*

undo rip output-delay

Default

An interface uses the RIP packet sending rate set for the RIP process that the interface runs.

Views

Interface view

Predefined user roles

network-admin

Parameters

Time: Specifies the RIP packet sending interval in the range of 10 to 100 milliseconds.

count: Specifies the maximum number of RIP packets sent at each interval, in the range of 1 to 30.

Examples

Configure VLAN-interface 10 to send a maximum of six RIP packets every 30 milliseconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip output-delay 30 count 6
```

Related commands

output-delay

rip poison-reverse

Use **rip poison-reverse** to enable the poison reverse feature.

Use **undo rip poison-reverse** to disable the poison reverse feature.

Syntax

rip poison-reverse

undo rip poison-reverse

Default

The poison reverse feature is disabled.

Views

Interface view

Predefined user roles

network-admin

Examples

Enable the poison reverse feature on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip poison-reverse
```

rip primary-path-detect bfd echo

Use **rip primary-path-detect bfd echo** to enable BFD single-hop echo detection for RIP FRR.

Use **undo rip primary-path-detect bfd** to disable BFD single-hop echo detection for RIP FRR.

Syntax

rip primary-path-detect bfd echo

undo rip primary-path-detect bfd

Default

BFD single-hop echo detection for RIP FRR is disabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

For quicker RIP FRR, use BFD single-hop echo detection on the primary link of redundant links to detect link failure.

Examples

Enable BFD single-hop echo detection for RIP FRR on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] fast-reroute route-policy frr
[Sysname-rip-1] quit
[Sysname] bfd echo-source-ip 1.1.1.1
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip primary-path-detect bfd echo
```

rip split-horizon

Use **rip split-horizon** to enable the split horizon feature.

Use **undo rip split-horizon** to disable the split horizon feature.

Syntax

rip split-horizon

undo rip split-horizon

Default

The split horizon feature is enabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

- The split horizon feature prevents routing loops. If you want to disable the feature, make sure the operation is necessary.
- If both split horizon and poison reverse are enabled, only the poison reverse feature takes effect.

Examples

Enable the split horizon feature on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip split-horizon
```

rip summary-address

Use **rip summary-address** to configure a summary route on an interface.

Use **undo rip summary-address** to remove a summary route on an interface.

Syntax

rip summary-address *ip-address* { *mask-length* | *mask* }

undo rip summary-address *ip-address* { *mask-length* | *mask* }

Default

No summary route is configured on an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the destination IP address of the summary route.

mask-length: Specifies the subnet mask length of the summary route, in the range of 0 to 32.

mask: Specifies the subnet mask of the summary route, in dotted decimal notation.

Usage guidelines

This command takes effect only when automatic route summarization is disabled.

Examples

Configure a summary route on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip summary-address 10.0.0.0 255.255.255.0
```

Related commands

summary

rip version

Use **rip version** to specify a RIP version on an interface.

Use **undo rip version** to restore the default.

Syntax

rip version { **1** | **2** [**broadcast** | **multicast**] }

undo rip version

Default

No RIP version is configured on an interface. The interface can send RIPv1 broadcasts, and receive RIPv1 broadcasts and unicasts, and RIPv2 broadcasts, multicasts, and unicasts.

Views

Interface view

Predefined user roles

network-admin

Parameters

1: Specifies the RIP version as RIPv1.

2: Specifies the RIP version as RIPv2.

[**broadcast** | **multicast**]: Sends RIPv2 messages in broadcast mode or multicast mode (default).

Usage guidelines

If an interface has no RIP version configured, it uses the global RIP version. Otherwise, it uses the RIP version configured on it.

An interface running RIPv1 can perform the following operations:

- Sends RIPv1 broadcast messages.
- Receives RIPv1 broadcast and unicast messages.

An interface running RIPv2 in broadcast mode can perform the following operations:

- Sends RIPv2 broadcast messages.
- Receives RIPv1 broadcast and unicast messages, and RIPv2 broadcast, multicast, and unicast messages.

An interface running RIPv2 in multicast mode can perform the following operations:

- Sends RIPv2 multicast messages.
- Receives RIPv2 broadcast, multicast, and unicast messages.

Examples

Configure RIPv2 in broadcast mode on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip version 2 broadcast
```

Related commands

version

silent-interface

Use **silent-interface** to disable interfaces from sending RIP messages. The interfaces can still receive RIP messages.

Use **undo silent-interface** to enable interfaces to send RIP messages.

Syntax

silent-interface { *interface-type interface-number* | **all** }

undo silent-interface { *interface-type interface-number* | **all** }

Default

All RIP interfaces can send RIP messages.

Views

RIP view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Disables a specified interface from sending RIP messages.

all: Disables all interfaces from sending RIP messages.

Examples

Disable all VLAN interfaces from sending RIP messages except VLAN-interface 10.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] silent-interface all
[Sysname-rip-100] undo silent-interface vlan-interface 10
[Sysname-rip-100] network 131.108.0.0
```

summary

Use **summary** to enable automatic RIPv2 route summarization. Natural masks are used to advertise summary routes to reduce the size of routing tables.

Use **undo summary** to disable automatic RIPv2 route summarization to advertise all subnet routes.

Syntax

summary

undo summary

Default

Automatic RIPv2 route summarization is enabled.

Views

RIP view

Predefined user roles

network-admin

Usage guidelines

Automatic RIPv2 route summarization can reduce the routing table size to enhance the scalability and efficiency for large networks.

Examples

Disable automatic RIPv2 route summarization.

```
<Sysname> system-view
[Sysname] rip
[Sysname-rip-1] undo summary
```

Related commands

rip summary-address

rip version

timer triggered

Use **timer triggered** to set the interval for sending triggered updates.

Use **undo timer triggered** to restore the default.

Syntax

timer triggered *maximum-interval* [*minimum-interval* [*incremental-interval*]]

undo timer triggered

Default

The maximum interval is 5 seconds, the minimum interval is 50 milliseconds, and the incremental interval is 200 milliseconds.

Views

RIP view

Predefined user roles

network-admin

Parameters

maximum-interval: Specifies the maximum interval in the range of 1 to 5 seconds.

minimum-interval: Specifies the minimum interval in the range of 10 to 5000 milliseconds.

incremental-interval: Specifies the incremental interval in the range of 100 to 1000 milliseconds.

Usage guidelines

The *minimum-interval* and *incremental-interval* cannot be greater than the *maximum-interval*.

For a stable network, the *minimum-interval* setting is used. If network changes become frequent, the incremental interval *incremental-interval* is used to extend the triggered update sending interval until the *maximum-interval* is reached.

Examples

For RIP process 1, set the maximum interval, minimum interval, and incremental interval to 2 seconds, 100 milliseconds, and 100 milliseconds, respectively.

```
<Sysname> system-view
```

```
[Sysname] rip 1
[Sysname-rip-1] timer triggered 2 100 100
```

timers

Use **timers** to set RIP timers.

Use **undo timers** to restore the default.

Syntax

timers { **garbage-collect** *garbage-collect-value* | **suppress** *suppress-value* | **timeout** *timeout-value* | **update** *update-value* } *

undo timers { **garbage-collect** | **suppress** | **timeout** | **update** } *

Default

The garbage-collect timer is 120 seconds, the suppress timer is 120 seconds, the timeout timer is 180 seconds, and the update timer is 30 seconds.

Views

RIP view

Predefined user roles

network-admin

Parameters

garbage-collect-value: Specifies the garbage-collect timer in the range of 1 to 3600 seconds.

suppress-value: Specifies the suppress timer in the range of 0 to 3600 seconds.

timeout-value: Specifies the timeout timer in the range of 1 to 3600 seconds.

update-value: Specifies the update timer in the range of 1 to 3600 seconds.

Usage guidelines

RIP uses the following timers:

- **Update timer**—Specifies the interval between routing updates.
- **Timeout timer**—Specifies the route aging time. If no update for a route is received before the timer expires, RIP sets the metric of the route to 16.
- **Suppress timer**—Specifies how long a RIP route stays in suppressed state. When the metric of a route becomes 16, the route enters the suppressed state. If RIP receives an update for the route with a metric less than 16 from the same neighbor, RIP uses this route to replace the suppressed route.
- **Garbage-collect timer**—Specifies the interval from when the metric of a route becomes 16 to when it is deleted from the routing table. During the garbage-collect timer length, RIP advertises the route with a metric of 16. If no update is announced for that route before the garbage-collect timer expires, RIP deletes the route from the routing table.

As a best practice, do not change the default values of these timers.

The timer lengths must be consistent on all routers on the network.

The timeout timer must be greater than the update timer.

Examples

Set the update, timeout, suppress, and garbage-collect timers to 5, 15, 15, and 30 seconds.

```
<Sysname> system-view
```

```
[Sysname] rip 100
[Sysname-rip-100] timers update 5 timeout 15 suppress 15 garbage-collect 30
```

validate-source-address

Use **validate-source-address** to enable source IP address check on inbound RIP routing updates.

Use **undo validate-source-address** to disable source IP address check on inbound RIP routing updates.

Syntax

validate-source-address

undo validate-source-address

Default

Source IP address check on inbound RIP routing updates is enabled.

Views

RIP view

Predefined user roles

network-admin

Examples

Disable source IP address check on inbound RIP routing updates.

```
<Sysname> system-view
[Sysname-rip] rip 100
[Sysname-rip-100] undo validate-source-address
```

version

Use **version** to specify a global RIP version.

Use **undo version** to restore the default.

Syntax

version { **1** | **2** }

undo version

Default

No global RIP version is configured. An RIP interface can send RIPv1 broadcasts and receive RIPv1 broadcasts and unicasts, and RIPv2 broadcasts, multicasts, and unicasts.

Views

RIP view

Predefined user roles

network-admin

Parameters

1: Specifies the RIP version as RIPv1.

2: Specifies the RIP version as RIPv2. RIPv2 messages are multicast.

Usage guidelines

An interface prefers the RIP version configured on it over the global RIP version.

If no RIP version is specified for the interface and the global version is RIPv1, the interface uses RIPv1 and can perform the following operations:

- Send RIPv1 broadcasts.
- Receive RIPv1 broadcasts and unicasts.

If no RIP version is specified for the interface and the global version is RIPv2, the interface uses RIPv2 multicast mode and can perform the following operations:

- Send RIPv2 multicasts.
- Receive RIPv2 broadcasts, multicasts, and unicasts.

Examples

Specify the global RIP version as RIPv2.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] version 2
```

Related commands

rip version

Contents

OSPF commands

The S5110V2-SI, S5000V3-EI, S5000V5-EI, S5000E-X, S5000X-EI, and WAS6000 switch series do not support OSPF.

abr-summary (OSPF area view)

Use **abr-summary** to configure route summarization on an ABR.

Use **undo abr-summary** to remove the configuration.

Syntax

abr-summary *ip-address* { *mask-length* | *mask* } [**advertise** | **not-advertise**] [**cost** *cost-value*]

undo abr-summary *ip-address* { *mask-length* | *mask* }

Default

Route summarization is not configured on an ABR.

Views

OSPF area view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the destination IP address of the summary route in dotted decimal notation.

mask-length: Specifies the mask length in the range of 0 to 32.

mask: Specifies the mask of the IP address, in dotted decimal notation.

advertise | **not-advertise**: Advertises the summary route or not. By default, the command advertises the summary route.

cost *cost-value*: Specifies the cost of the summary route, in the range of 1 to 16777215. The default cost is the largest cost value among routes that are summarized.

Usage guidelines

This command applies only to an ABR to summarize multiple contiguous networks into one network.

To enable ABR to advertise specific routes that have been summarized, use the **undo abr-summary** command.

Examples

Summarize networks 36.42.10.0/24 and 36.42.110.0/24 in Area 1 into 36.42.0.0/16.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] network 36.42.10.0 0.0.0.255
[Sysname-ospf-100-area-0.0.0.1] network 36.42.110.0 0.0.0.255
[Sysname-ospf-100-area-0.0.0.1] abr-summary 36.42.0.0 255.255.0.0
```

area (OSPF view)

Use **area** to create an OSPF area and enter OSPF area view.

Use **undo area** to remove an OSPF area.

Syntax

area *area-id*

undo area *area-id*

Default

No OSPF areas exist.

Views

OSPF view

Predefined user roles

network-admin

Parameters

area-id: Specifies an area by its ID, an IP address or a decimal integer in the range of 0 to 4294967295 that is translated into the IP address format.

Examples

Create Area 0 and enter Area 0 view.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 0
[Sysname-ospf-100-area-0.0.0.0]
```

asbr-summary (OSPF view)

Use **asbr-summary** to configure route summarization on an ASBR.

Use **undo asbr-summary** to remove the configuration.

Syntax

asbr-summary *ip-address* { *mask-length* | *mask* } [**cost** *cost-value* | **not-advertise** | **nssa-only** | **tag** *tag*] *

undo asbr-summary *ip-address* { *mask-length* | *mask* }

Default

Route summarization is not configured on an ASBR.

Views

OSPF view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the destination IP address of the summary route.

mask-length: Specifies the mask length in the range of 0 to 32.

mask: Specifies the mask in dotted decimal notation.

cost *cost-value*: Specifies the cost of the summary route, in the range of 1 to 16777214. If you do not specify this option, the largest cost among the summarized routes applies. If the routes in Type-5 LSAs translated from Type-7 LSAs are Type-2 external routes, the largest cost among the summarized routes plus 1 applies.

not-advertise: Disables advertising the summary route. If you do not specify this keyword, the command advertises the route.

nssa-only: Limits the route advertisement to the NSSA area by setting the P-bit of Type-7 LSAs to 0. By default, the P-bit of Type-7 LSAs is set to 1. If the ASBR is also an ABR and **FULL** state neighbors exist in the backbone area, the P-bit of Type-7 LSAs originated by the ASBR is set to 0. This keyword applies to the NSSA ASBR.

tag *tag*: Specifies a tag for the summary route, in the range of 0 to 4294967295. The default is 1. The tag can be used by a routing policy to control summary route advertisement.

Usage guidelines

An ASBR can summarize routes in the following LSAs:

- Type-5 LSAs.
- Type-7 LSAs in an NSSA area.
- Type-5 LSAs translated by the ASBR (also an ABR) from Type-7 LSAs in an NSSA area.

  If the ASBR (ABR) is not a translator, it cannot summarize routes in Type-5 LSAs translated from Type-7 LSAs.

To enable ASBR to advertise specific routes that have been summarized, use the **undo asbr-summary** command.

Examples

Summarize redistributed static routes into a single route, and specify a tag value of 2 and a cost of 100 for the summary route.

```
<Sysname> system-view
[Sysname] ip route-static 10.2.1.0 24 null 0
[Sysname] ip route-static 10.2.2.0 24 null 0
[Sysname] ospf 100
[Sysname-ospf-100] import-route static
[Sysname-ospf-100] asbr-summary 10.2.0.0 255.255.0.0 tag 2 cost 100
```

authentication-mode

Use **authentication-mode** to specify an authentication mode for an OSPF area.

Use **undo authentication-mode** to remove the configuration.

Syntax

For MD5/HMAC-MD5 authentication:

authentication-mode { **hmac-md5** | **md5** } *key-id* { **cipher** | **plain** } *string*

undo authentication-mode [{ **hmac-md5** | **md5** } *key-id*]

For simple authentication:

authentication-mode simple { **cipher** | **plain** } *string*

undo authentication-mode

Default

No authentication is performed for an area.

Views

OSPF area view

Predefined user roles

network-admin

Parameters

hmac-md5: Specifies the HMAC-MD5 authentication mode.

md5: Specifies the MD5 authentication mode.

simple: Specifies the simple authentication mode.

key-id: Specifies a key by its ID in the range of 0 to 255.

cipher: Specifies a key in encrypted form.

plain: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive.

- In simple authentication mode, the plaintext form of the key is a string of 1 to 8 characters. The encrypted form of the key is a string of 33 to 41 characters.
- In MD5/HMAC-MD5 authentication mode, the plaintext form of the key is a string of 1 to 16 characters. The encrypted form of the key is a string of 33 to 53 characters.

Usage guidelines

To establish or maintain adjacencies, routers in the same area must have the same authentication mode and key.

If MD5 or HMAC-MD5 authentication is configured, you can configure multiple keys, each having a unique key ID and key string. As a best practice to minimize the risk of key compromise, use only one key for an area and delete the old key after key replacement.

To replace the key used for MD5 or HMAC-MD5 authentication in an area, you must configure the new key before removing the old key from each router. OSPF uses the key rollover mechanism to ensure that the routers can pass authentication before the replacement is complete across the area. After you configure a new key on a router, the router sends copies of the same packet, each authenticated by a different key, including the new key and the keys in use. This practice continues until the router detects that all its neighbors have the new key.

Examples

Configure OSPF Area 0 to use the MD5 authentication mode, and set the key ID to 15 and the key to **abc** in plaintext form.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 0
[Sysname-ospf-100-area-0.0.0.0] authentication-mode md5 15 plain abc
```

Related commands

ospf authentication-mode

bandwidth-reference (OSPF view)

Use **bandwidth-reference** to set a reference bandwidth value for link cost calculation.

Use **undo bandwidth-reference** to restore the default value.

Syntax

bandwidth-reference *value*

undo bandwidth-reference

Default

The reference bandwidth value is 100 Mbps for link cost calculation.

Views

OSPF view

Predefined user roles

network-admin

Parameters

value: Specifies the reference bandwidth value for link cost calculation, in the range of 1 to 4294967 Mbps.

Usage guidelines

If no cost values are configured for links, OSPF calculates their cost values by using the following formula: Cost = Reference bandwidth value / Expected interface bandwidth. The expected bandwidth of an interface is configured with the **bandwidth** command (see *Interface Command Reference*). If the calculated cost is greater than 65535, the value of 65535 is used. If the calculated cost is less than 1, the value of 1 is used.

Examples

Set the reference bandwidth value to 1000 Mbps.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] bandwidth-reference 1000
```

Related commands

ospf cost

capability default-exclusion

Use **capability default-exclusion** to exclude interfaces in an OSPF area from the base topology.

Use **undo capability default-exclusion** to restore the default.

Syntax

capability default-exclusion

undo capability default-exclusion

Default

Interfaces in an OSPF area belong to the base topology.

Views

OSPF area view

Predefined user roles

network-admin

Usage guidelines

For correct neighbor relationship establishment, execute this command on both the local device and the neighbor device.

Examples

Exclude interfaces in Area 1 from the base topology.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] capability default-exclusion
```

database-filter peer (OSPF view)

Use **database-filter peer** to filter LSAs for the specified P2MP neighbor.

Use **undo database-filter peer** to restore the default.

Syntax

database-filter peer *ip-address* { **all** | { **ase** [**acl** *ipv4-acl-number*] | **nssa** [**acl** *ipv4-acl-number*] | **summary** [**acl** *ipv4-acl-number*] } * }

undo database-filter peer *ip-address*

Default

The LSAs for the specified P2MP neighbor are not filtered.

Views

OSPF view

Predefined user roles

network-admin

Parameters

ip-address: Specifies a P2MP neighbor by its IP address.

all: Filters all LSAs except the Grace LSAs.

ase: Filters Type-5 LSAs.

nssa: Filters Type-7 LSAs.

summary: Filters Type-3 LSAs.

acl *ipv4-acl-number*: Specifies an IPv4 ACL by its number in the range of 2000 to 3999.

Usage guidelines

On an P2MP network, a router might have multiple OSPF neighbors with the P2MP type. Use this command to prevent the router from sending LSAs to the specified neighbor.

To use an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL using one of the following methods:

- To deny/permit LSAs with the specified link state ID, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* command.
- To deny/permit LSAs with the specified link state ID and mask, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* **destination** *dest-addr dest-wildcard* command.

The **source** keyword specifies the link state ID of an LSA and the **destination** keyword specifies the subnet mask of the LSA. For the mask configuration to take effect, specify a contiguous subnet mask.

If the specified neighbor has already received an LSA, the LSA still exists in the LSDB of the neighbor after you execute the command.

Examples

Filter all LSAs (except the Grace LSAs) for the P2MP neighbor with the IP address 121.20.20.121.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] database-filter peer 121.20.20.121 all
```

Configure advanced ACL 3000 to filter Type-3 LSAs for the P2MP neighbor with the IP address 121.20.20.121.

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule 10 deny ip source 121.20.0.0 0 destination 255.255.0.0
0
[Sysname-acl-ipv4-adv-3000] rule 100 permit ip
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] ospf 1
[Sysname-ospf-1] database-filter peer 121.20.20.121 summary acl 3000
```

Related commands

ospf database-filter

default (OSPF view)

Use **default** to configure default parameters for redistributed routes.

Use **undo default** to remove the configuration.

Syntax

default { **cost** *cost-value* | **tag** *tag* | **type** *type* } *

undo default { **cost** | **tag** | **type** } *

Default

The cost is 1, the tag is 1, and the route type is 2.

Views

OSPF view

Predefined user roles

network-admin

Parameters

cost *cost-value*: Specifies a default cost for redistributed routes, in the range of 0 to 16777214.

tag *tag*: Specifies a tag for redistributed routes, in the range of 0 to 4294967295.

type *type*: Specifies a type for redistributed routes: 1 or 2.

Examples

Set the default cost, tag, and type to 10, 100, and 2 for redistributed external routes.

```
<Sysname> system-view
```

```
[Sysname] ospf 100
[Sysname-ospf-100] default cost 10 tag 100 type 2
```

Related commands

import-route

default-cost (OSPF area view)

Use **default-cost** to set a cost for the default route advertised to the stub or NSSA area.

Use **undo default-cost** to restore the default value.

Syntax

default-cost *cost-value*

undo default-cost

Default

The cost is 1.

Views

OSPF area view

Predefined user roles

network-admin

Parameters

cost-value: Specifies a cost for the default route advertised to the Stub or NSSA area, in the range of 0 to 16777214.

Usage guidelines

This command takes effect only on the ABR of a stub area or the ABR or ASBR of an NSSA area.

Examples

Configure Area 1 as a stub area, and set the cost of the default route advertised to the stub area to 20.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] stub
[Sysname-ospf-100-area-0.0.0.1] default-cost 20
```

Related commands

nssa

stub

default-route-advertise (OSPF view)

Use **default-route-advertise** to redistribute a default route into the OSPF routing domain.

Use **undo default-route-advertise** to restore the default.

Syntax

default-route-advertise [[**always** | **permit-calculate-other**] | **cost** *cost-value* | **route-policy** *route-policy-name* | **type** *type*] *

undo default-route-advertise

Default

No default route is redistributed into the OSPF routing domain.

Views

OSPF view

Predefined user roles

network-admin

Parameters

always: Redistributes a default route in a Type-5 LSA into the OSPF routing domain regardless of whether a default route exists in the routing table. If you do not specify this keyword, the router redistributes a default route only when an active default route that does not belong to the current OSPF process exists in the IP routing table.

permit-calculate-other: Enables OSPF to calculate default routes received from other routers. If you do not specify this keyword, OSPF does not calculate default routes from other routers. If the router does not redistribute any default route in a Type-5 LSA into the OSPF routing domain, the router calculates default routes from other routers. It calculates these routes regardless of whether this keyword is specified.

cost *cost-value*: Specifies a cost for the default route, in the range of 0 to 16777214. If you do not specify this option, the default cost specified by the **default-cost** command applies.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters. When the routing policy is matched and one of the following conditions is met, the command redistributes a default route in a Type-5 LSA into the OSPF routing domain:

- A default route exists in the routing table.
- The **always** keyword is specified.

The routing policy modifies values in the Type-5 LSA.

type *type*: Specifies a type for the Type-5 LSA: 1 or 2. If you do not specify this option, the default type for the Type-5 LSA specified by the **default type** command applies.

Usage guidelines

This command redistributes a default route in a Type-5 LSA, which cannot be redistributed with the **import-route** command. If the local routing table has no default route, you must specify the **always** keyword for the command.

Examples

Redistribute a default route into the OSPF routing domain, regardless of whether the default route exists in the local routing table.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] default-route-advertise always
```

Related commands

default

import-route

description (OSPF/OSPF area view)

Use **description** to configure a description for an OSPF process or area.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

No description is configured for an OSPF process or area.

Views

OSPF view

OSPF area view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 80 characters.

Usage guidelines

The description specified by this command is used to identify an OSPF process or area.

Examples

Describe OSPF process 100 as **abc**.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] description abc
```

Describe OSPF Area 0 as **bone area**.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 0
[Sysname-ospf-100-area-0.0.0.0] description bone area
```

discard-route

Use **discard-route** to configure discard routes for summary networks.

Use **undo discard-route** to restore the default.

Syntax

discard-route { **external** { *preference* | **suppression** } | **internal** { *preference* | **suppression** } } *

undo discard-route [**external** | **internal**] *

Default

A device generates discard routes with preference 255 for summary networks.

Views

OSPF view

Predefined user roles

network-admin

Parameters

external: Specifies discard routes for redistributed summary networks on the ASBR. These discard routes are external discard routes.

preference: Specifies a preference for external discard routes, in the range of 1 to 255.

suppression: Disables the ASBR from generating external discard routes for summary networks.

internal: Specifies discard routes for summary networks on the ABR. These discard routes are internal discard routes.

preference: Specifies a preference for internal discard routes, in the range of 1 to 255.

suppression: Disables the ABR from generating internal discard routes for summary networks.

Examples

Generate external and internal discard routes with preference 100 and 200, respectively.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] discard-route external 100 internal 200
```

display ospf

Use **display ospf** to display OSPF process information.

Syntax

display ospf [*process-id*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays information about all OSPF processes.

verbose: Displays detailed OSPF process information. If you do not specify this keyword, the command displays brief OSPF process information.

Examples

Display detailed OSPF process information.

```
<Sysname> display ospf verbose

          OSPF Process 1 with Router ID 192.168.1.2
                 OSPF Protocol Information

 RouterID: 192.168.1.2      Router type:  NSSA
 Route tag: 0
 Multi-VPN-Instance is not enabled
 Ext-community type: domain ID 0x105, route type 0x8000, router ID 0x8001
 Domain ID: 0.0.0.0:23
 Opaque capable
```

```
Originating router-LSAs with maximum metric
   Condition: On startup for 600 seconds, State: Inactive
   Advertise stub links with maximum metric in router-LSAs
   Advertise summary-LSAs with metric 16711680
   Advertise external-LSAs with metric 16711680
ISPF is enabled
SPF-schedule-interval: 5 50 200
LSA generation interval: 5
LSA arrival interval: 1000
Transmit pacing: Interval: 20 Count: 3
Default ASE parameters: Metric: 1 Tag: 1 Type: 2
Route preference: 10
ASE route preference: 150
SPF computation count: 22
RFC 1583 compatible
Graceful restart interval: 120
SNMP trap rate limit interval: 2  Count: 300
This process is currently bound to MIB
Area count: 1   NSSA area count: 1
Normal areas with up interfaces: 0
NSSA areas with up interfaces: 1
Up interfaces: 1
ExChange/Loading neighbors: 0
Full neighbors:3
Area0 full neighbors: 1
Calculation trigger type: Full
Current calculation type: SPF calculation
Current calculation phase: Calculation area topology
Process reset state: N/A
Current reset type: N/A
Next reset type: N/A
Reset prepare message replied: -/-/-/-
Reset process message replied: -/-/-/-
Reset phase of module:
  M-N/A, P-N/A, L-N/A, C-N/A, R-N/A

Area: 0.0.0.1          (MPLS TE not enabled)
Authtype: None    Area flag: NSSA
7/5 translator state: Disabled
7/5 translate stability timer interval: 0
SPF scheduled count: 5
ExChange/Loading neighbors: 0
Up interfaces: 1

Interface: 192.168.1.2 (Vlan-interface10)
Cost: 1       State: DR        Type: Broadcast    MTU: 1500
Priority: 1
Designated router: 192.168.1.2
```

```
Backup designated router: 192.168.1.1
Timers: Hello 10 , Dead 40 , Poll  40 , Retransmit 5 , Transmit Delay 1
FRR backup: Enabled
Enabled by network configuration
Packet size: 1000
```

Table 1 Command output

Field	Description
OSPF Process 1 with Router ID 192.168.1.2	OSPF process ID and OSPF router ID.
RouterID	Router ID.
Router type	Router type: • ABR. • ASBR. • NSSA. • Null.
Route tag	Tag of redistributed routes.
Multi-VPN-Instance is not enabled	The OSPF process does not support multi-VPN-instance.
Ext-community type	OSPF extended community attribute type codes: • **Domain ID**—Domain ID code. • **Route Type**—Router type code. • **Router ID**—Router ID code.
Domain ID	OSPF domain ID (primary ID).
Opaque capable	Opaque LSA advertisement and reception capability is enabled.
Originating router-LSAs with maximum metric	The maximum cost value for router LSAs (excluding stub links) is used.
Condition	Status of the stub router: • Always. • On startup for *xxx* seconds, where *xxx* is specified by the user.
State	Whether the stub router is active.
SPF-schedule-interval	Interval for SPF calculations.
LSA generation interval	LSA generation interval.
LSA arrival interval	LSA arrival interval.
Transmit pacing	LSU packet transmit rate of the interface: • **Interval**—LSU transmit interval of the interface. • **Count**—Maximum number of LSU packets sent at each interval.
Default ASE parameters	Default ASE parameters: **Metric**, **Tag**, and **Type**.
Route preference	Internal route preference.
ASE route preference	External route preference.
SPF computation count	SPF computation count of the OSPF process.
RFC1583 compatible	Compatible with RFC 1583.

Graceful restart interval	GR interval.
SNMP trap rate limit interval	SNMP notification sending interval.
Count	Number of sent SNMP notifications.
ExChange/Loading neighbors	Neighbors in ExChange/Loading state.
Full neighbors	Neighbors in Full state.
Area0 full neighbors	Neighbors in Full state in the backbone area.
Calculation trigger type	Route calculation trigger type: • **Full**—Calculation of all routes is triggered. • **Area topology change**—Topology change in an area. • **Intra router change**—Incremental intra-area route change. • **ASBR change**—Incremental ASBR route change. • **7to5 translator**—Type-7-to-Type-5 LSA translator role change. • **Full IP prefix**—Calculation of all IP prefixes is triggered. • **Full intra AS**—Calculation of all intra-AS prefixes is triggered. • **Inc intra AS**—Calculation of incremental intra-AS prefixes is triggered. • **Full inter AS**—Calculation of all AS-external prefixes is triggered. • **Inc inter AS**—Calculation of incremental AS-external prefixes is triggered. • **N/A**—Route calculation is not triggered.
Current calculation type	Current route calculation type: • SPF calculation. • **Intra router calculation**—Intra-area route calculation. • **ASBR calculation**—Inter-area ASBR route calculation. • **Inc intra router**—Incremental intra-area route calculation. • **Inc ASBR calculation**—Incremental inter-area ASBR route calculation. • **7to5 translator**—Type-7-to-Type-5 LSA calculation. • **Full intra AS**—Calculation of all intra-AS prefixes. • **Inc intra AS**—Calculation of incremental intra-AS prefixes. • **Full inter AS**—Calculation of all AS-external prefixes. • **Inc inter AS**—Calculation of incremental AS-external prefixes. • **Forward address**—Forwarding address calculation. • **N/A**—Route calculation is not triggered.
Current calculation phase	Current route calculation phase: • **Calculation area topology**—Calculating area topology. • **Calculation router**—Calculating routes on routers. • **Calculation intra AS**—Calculating intra-AS routes. • **7to5 translator**—Calculating Type-7-to-Type-5 LSAs. • **Forward address**—Calculating forwarding addresses. • **Calculation inter AS**—Calculating AS-external routes. • **Calculation end**—Ending phase of calculation. • **N/A**—Route calculation is not triggered.

Process reset state	Process reset state: • **N/A**—The process is not reset. • **Under reset**—The process is in the reset progress. • **Under RIB smooth**—The process is synchronizing the RIB.
Current reset type	Current process reset type: • **N/A**—The process is not reset. • **Normal**—Normal reset. • **GR quit**—Normal reset when GR quits abnormally. • **Delete**—Delete OSPF process.
Next reset type	Next process reset type: • **N/A**—The process is not reset. • **Normal**—Normal reset. • **GR quit**—Normal reset when GR quits abnormally. • **Delete**—Delete OSPF process.
Reset prepare message replied	Modules that reply reset prepare messages: • **P**—Neighbor maintenance module. • **L**—LSDB synchronization module. • **C**—Route calculation module. • **R**—Route redistribution module.
Reset process message replied	Modules that reply reset process messages: • **P**—Neighbor maintenance module. • **L**—LSDB synchronization module. • **C**—Route calculation module. • **R**—Route redistribution module.

Reset phase of module	Reset phase of each module:
	• Main control module:
	  ○ **N/A**—Not reset.
	  ○ Delete area.
	  ○ Delete process.
	• Neighbor maintenance (P) module:
	  ○ **N/A**—Not reset.
	  ○ Delete neighbor.
	  ○ Delete interface.
	  ○ **Delete vlink**—Delete virtual link.
	• LSDB synchronization (L) module:
	  ○ **N/A**—Not reset.
	  ○ Stop timer.
	  ○ **Delete ASE**—Delete all ASE LSAs.
	  ○ **Delete ASE maps**—Delete ASE LSA maps.
	  ○ Clear process data.
	  ○ **Delete area LSA**—Delete LSAs and maps from an area.
	  ○ **Delete area interface**—Delete interfaces from an area.
	  ○ **Delete process**—Delete process-related resources.
	  ○ **Restart**—Restart process-related resources.
	• Route calculation (C) module:
	  ○ **N/A**—Not reset.
	  ○ **Delete topology**—Delete area topology.
	  ○ **Delete router**—Delete routes of routers.

	○ **Delete intra AS**—Delete intra-AS routes ○ **Delete inter AS**—Delete AS-external routes. ○ **Delete forward address**—Delete forwarding address list. ○ **Delete advertise**—Delete advertising router list. • Route redistribution (R) module: ○ **N/A**—Not reset. ○ **Delete ABR summary**—Delete summary routes of the ABR. ○ **Delete ASBR summary**—Delete summary routes of the ASBR. ○ **Delete import**—Delete redistributed routes.
Area	Area ID in the IP address format.
MPLS TE not enabled	Status of MPLS TE for the OSPF area, which can be **MPLS TE not enabled** or **MPLS TE enabled**.
Authtype	Authentication type of the area: • **None**—No authentication. • **Simple**—Simple authentication. • **MD5**—MD5 authentication.
Area flag	Type of the area: • Normal. • Stub. • StubNoSummary (totally stub area). • NSSA. • NSSANoSummary (totally NSSA area).
7/5 translator state	State of the translator that translates Type-7 LSAs to Type-5 LSAs: • **Enabled**—The translator is specified through commands. • **Elected**—The translator is designated through election. • **Disabled**—The device is not a translator.
7/5 translate stability timer interval	Stability interval for Type-7 LSA-to-Type-5 LSA translation.
SPF scheduled Count	SPF calculation count in the OSPF area.
Interface	Interface in the area.
Cost	Interface cost.
State	Interface state.
Type	Interface network type.
MTU	Interface MTU.
Priority	Router priority.
Timers	OSPF timers: • **Hello**—Interval for sending hello packets. • **Dead**—Interval within which the neighbor is down. • **Poll**—Interval for sending hello packets. • **Retransmit**—Interval for retransmitting LSAs.
FRR backup	Whether Loop Free Alternate (LFA) calculation is enabled on an interface.
Enabled by interface configuration (including secondary IP addresses)	OSPF is enabled on the interface. **including secondary IP addresses** indicates that OSPF advertises the direct routes

	to the primary and secondary addressess of the interface.
Simple authentication enabled	Simple authentication is enabled.
MD5 authentication enabled	MD5/HMAC-MD5 authentication is enabled.
The last key is *xx*	The most recent MD5/HMAC-MD5 authentication key ID is *xx*.
The rollover is in progress, *xx* neighbor(s) left	Key rollover for MD5/HMAC-MD5 authentication is in progress. The number of neighbors that have not completed rollover is *xx*.
Packet size	Maximum length of OSPF packets that can be sent by the interface.

display ospf abr-asbr

Use **display ospf abr-asbr** to display routes to the ABR or ASBR.

Syntax

display ospf [*process-id*] **abr-asbr** [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays routes to the ABR and ASBR for all OSPF processes.

verbose: Displays detailed information. If you do not specify this keyword, the command displays brief information.

Usage guidelines

If you use this command on routers in a stub area, the commands displays no ASBR information.

Examples

Display brief information about routes to the ABR or ASBR.

```
<Sysname> display ospf abr-asbr

          OSPF Process 1 with Router ID 192.168.1.2
                  Routing Table to ABR and ASBR


                 Topology base (MTID 0)
 Type        Destination       Area       Cost  Nexthop         RtType
 Inter       3.3.3.3           0.0.0.0    3124  10.1.1.2        ASBR
 Intra       2.2.2.2           0.0.0.0    1562  10.1.1.2        ABR
```

Display detailed information about routes to the ABR or ASBR.

```
<Sysname> display ospf abr-asbr verbose

          OSPF Process 10 with Router ID 101.1.1.11
```

```
                  Routing Table to ABR and ASBR

                Topology base (MTID 0)

Destination: 1.1.1.1            RtType     : ASBR
Area       : 0.0.0.1            Type       : Intra
Nexthop    : 150.0.1.12         BkNexthop  : 0.0.0.0
Interface  : Vlan10             BkInterface: N/A
Cost       : 1000
```

Table 2 Command output

Field	Description
Type	Type of the route to the ABR or ASBR: • **Intra**—Intra-area route. • **Inter**—Inter-area route.
Topology	Topology name. The topology name for base topology is **base**.
MTID	Topology ID. The value of 0 indicates the base topology.
Destination	Router ID of an ABR or ASBR.
Area	ID of the area of the next hop.
Cost	Cost from the router to the ABR or ASBR.
Nexthop	Next hop address.
BkNexthop	Backup next hop address.
RtType	Router type: ABR or ASBR.
Interface	Output interface.
BkInterface	Backup output interface.

display ospf abr-summary

Use **display ospf abr-summary** to display ABR summary route information.

Syntax

display ospf [*process-id*] [**area** *area-id*] **abr-summary** [*ip-address* { *mask-length* | *mask* }] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays information about ABR summary routes for all OSPF processes.

area *area-id*: Specifies an OSPF area by its ID. The area ID is an IP address or a decimal integer in the range of 0 to 4294967295 that is translated into the IP address format. If you do not specify this option, the command displays information about ABR summary routes for all OSPF areas.

ip-address: Specifies a summary route by its IP address.

mask-length: Specifies the mask length in the range of 0 to 32.

mask: Specifies the mask in dotted decimal notation.

verbose: Displays detailed ABR summary route information. If you do not specify this keyword, the command displays brief ABR summary route information.

Usage guidelines

If you do not specify an IP address, this command displays information about all summary routes on the ABR.

Examples

Display brief information about summary routes on the ABR.

```
<Sysname> display ospf abr-summary

          OSPF Process 1 with Router ID 2.2.2.2
                  ABR Summary Addresses

                Topology base (MTID 0)
                        Area: 0.0.0.1
 Total summary address count: 1
 Net             Mask            Status        Count      Cost
 100.0.0.0       255.0.0.0       Advertise     1          (Not Configured)
```

Table 3 Command output

Field	Description
Topology	Topology name. The topology name for base topology is **base**.
MTID	Topology ID. The value of 0 indicates the base topology.
Area	Area to which the summary routes belong.
Total summary address count	Total number of summary routes.
Net	Address of the summary route.
Mask	Mask of the summary route address.
Status	Advertisement status of the summary route: **Advertise** or **Non-Advertise**.
Count	Number of summarized routes.
Cost	Cost of the summary route.

Display detailed information about summary routes on the ABR.

```
<Sysname> display ospf abr-summary verbose

          OSPF Process 1 with Router ID 2.2.2.2
                  ABR Summary Addresses

                Topology base (MTID 0)
```

```
                        Area: 0.0.0.1
 Total summary address count: 1

 Net         : 100.0.0.0
 Mask        : 255.0.0.0
 Status      : Advertise
 Cost        : (Not Configured)
 Routes count: 1
   Destination            NetMask                Metric
   100.1.1.0              255.255.255.0          1000
```

Table 4 Command output

Field	Description
Topology	Topology name. The topology name for base topology is **base**.
MTID	Topology ID. The value of 0 indicates the base topology.
Destination	Destination address of a summarized route.
NetMask	Network mask of a summarized route.
Metric	Metric of a summarized route.

display ospf asbr-summary

Use **display ospf asbr-summary** to display ASBR summary route information.

Syntax

display ospf [*process-id*] **asbr-summary** [*ip-address* { *mask-length* | *mask* }]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays information about ASBR summary routes for all OSPF processes.

ip-address: Specifies an IP address in dotted decimal notation.

mask-length: Specifies the mask length in the range of 0 to 32.

mask: Specifies the mask in dotted decimal notation.

Usage guidelines

If you do not specify an IP address, this command displays information about all ASBR summary routes.

Examples

Display ASBR summary route information in OSPF process 1.

```
<Sysname> display ospf 1 asbr-summary

          OSPF Process 1 with Router ID 2.2.2.2
                  Summary Addresses


               Topology base (MTID 0)
 Total summary address count: 1

                  Summary Address

 Net         : 30.1.0.0
 Mask        : 255.255.0.0
 Tag         : 20
 Status      : Advertise
 Cost        : 10 (Configured)
 Route count : 2

 Destination     Net mask        Proto      Process   Type     Metric

 30.1.2.0        255.255.255.0   OSPF       2         2        1
 30.1.1.0        255.255.255.0   OSPF       2         2        1
```

Table 5 Command output

Field	Description
Topology	Topology name. The topology name for base topology is **base**.
MTID	Topology ID. The value of 0 indicates the base topology.
Total summary address count	Total number of summary routes.
Net	Address of the summary route.
Mask	Mask of the summary route address.
Tag	Tag of the summary route.
Status	Advertisement status of the summary route.
Cost	Cost of the summary route.
Route count	Number of summarized routes.
Destination	Destination address of a summarized route.
Net mask	Network mask of a summarized route.
Proto	Routing protocol from which the route was redistributed.
Process	Process ID of the routing protocol from which the route was redistributed.
Type	Type of a summarized route.
Metric	Metric of a summarized route.

display ospf event-log

Use **display ospf event-log** to display OSPF log information.

Syntax

display ospf [*process-id*] **event-log** { **lsa-flush** | **peer** | **spf** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays OSPF log information for all processes.

lsa-flush: Specifies LSA aging log information.

peer: Specifies neighbor log information.

spf: Specifies route calculation log information.

Usage guidelines

Route calculation logs show the number of routes newly installed in the IP routing table.

Neighbor logs include information about the following events:

- The OSPF neighbor state goes down.
- The OSPF neighbor state goes backward because the local end receives BadLSReq, SeqNumberMismatch, and 1-Way events.

Examples

Display OSPF LSA aging log information for all processes.

```
<Sysname> display ospf event-log lsa-flush

          OSPF Process 1 with Router ID 1.1.1.1
                  LSA Flush Log

 Date: 2013-09-22 Time: 14:47:33 Received MaxAge LSA from 10.1.1.1
 Type: 1   LS ID: 2.2.2.2         AdvRtr: 2.2.2.2           Seq#: 80000001

 Date: 2013-09-22 Time: 14:47:33 Flushed MaxAge LSA by the self
 Type: 1   LS ID: 1.1.1.1         AdvRtr: 1.1.1.1           Seq#: 80000001

 Date: 2013-09-22 Time: 14:47:33 Received MaxAge LSA from 10.1.2.2
 Type: 1   LS ID: 2.2.2.2         AdvRtr: 2.2.2.2           Seq#: 80000001

 Date: 2013-09-22 Time: 14:47:33 Flushed MaxAge LSA by the self
 Type: 1   LS ID: 1.1.1.1         AdvRtr: 1.1.1.1           Seq#: 80000001
```

Table 6 Command output

Field	Description
Date/Time	Time when the device receives an LSA that has reached the maximum age.
Received MaxAge LSA from *X.X.X.X*	The device received an LSA that has reached the maximum age from *X.X.X.X*.
Flushed MaxAge LSA by the self	The device flushed the LSA that has reached the maximum age.
Type	LSA type.
LS ID	LSA link state ID.
AdvRtr	Advertising router.
Seq#	LSA sequence number.

Display OSPF route calculation log information for all processes.

```
<Sysname> display ospf event-log spf

          OSPF Process 1 with Router ID 1.1.1.2
                  SPF Log

               Topology base (MTID 0)

Date       Time     Duration   Intra Inter External Reason
2012-06-27 15:28:26 0.95       1     1     10000    Intra-area LSA
2012-06-27 15:28:23 0.2        0     0     0        Area 0 full neighbor
2012-06-27 15:28:19 0          0     0     0        Intra-area LSA
2012-06-27 15:28:19 0          0     0     0        external LSA
2012-06-27 15:28:19 0.3        0     0     0        Intra-area LSA
2012-06-27 15:28:12 0          1     0     0        Intra-area LSA
2012-06-27 15:28:11 0          0     0     0        Routing policy
2012-06-27 15:28:11 0          0     0     0        Intra-area LSA
```

Table 7 Command output

Field	Description
Topology	Topology name. The topology name for base topology is **base**.
MTID	Topology ID. The value of 0 indicates the base topology.
Date/Time	Time when the route calculation starts.
Duration	Duration of the route calculation, in seconds.
Intra	Number of intra-area routes newly installed in the IP routing table.
Inter	Number of inter-area routes newly installed in the IP routing table.
External	Number of external routes newly installed in the IP routing table.
Reason	Reasons why the route calculation is performed: • **Intra-area LSA**—Intra-area LSA changes. • **Inter-area LSA**—Inter-area LSA changes. • **External LSA**—External LSA changes. • **Configuration**—Configuration changes.

	• **Area 0 full neighbor**—Number of **FULL**-state neighbors in Area 0 changes. • **Area 0 up interface**—Number of interfaces in up state in Area 0 changes. • **LSDB overflow state**—Overflow status changes. • **AS number**—AS number changes. • **ABR summarization**—ABR summarization changes. • **GR end**—GR ends. • **Routing policy**—Routing policy changes. • **Others**—Other reasons.

Display OSPF neighbor log information for OSPF process 1.

```
<Sysname> display ospf 1 event-log peer

          OSPF Process 1 with Router ID 1.1.1.1
                  Neighbors Log

Date       Time     Local Address   Remote Address  Router ID       Reason
2012-12-31 12:35:45 197.168.1.1     197.168.1.2     2.2.2.2         IntPhyChange
2012-12-31 12:35:19 197.168.1.1     197.168.1.2     2.2.2.2         ConfNssaArea
2012-12-31 12:34:59 197.168.1.1     197.168.1.2     2.2.2.2         SilentInt
```

Table 8 Command output

Field	Description
Date/Time	Time when the neighbor state changes.
Local Address	Local address of the neighbor relationship.
Remote Address	Peer address of the neighbor relationship.
Router ID	Neighbor router ID.
Reason	Reasons for neighbor state changes: • **ResetConnect**—The connection is lost due to insufficient memory. • **IntChange**—The interface parameter has changed. • **VlinkChange**—The virtual link parameter has changed. • **ResetOspf**—The OSPF process is reset. • **UndoOspf**—The OSPF process is deleted. • **UndoArea**—The OSPF area is deleted. • **UndoNetwork**—The interface is disabled. • **SilentInt**—The interface is configured as a silent interface. • **IntLogChange**—The logical attribute of the interface has changed. • **IntPhyChange**—The physical attribute of the interface has changed. • **IntVliChange**—The virtual link attribute of the interface has changed. • **VlinkDown**—The virtual link goes down. • **DeadExpired**—The dead timer expires. • **ConfStubArea**—The interface is configured with stub area parameters. • **ConfNssaArea**—The interface is configured with NSSA area parameters. • **AuthChange**—The authentication type has changed. • **OpaqueChange**—The Opaque capability has changed. • **Retrans**—Excessive retransmissions. • **LLSChange**—The LLS capability has changed.

	• **OOBChange**—The OOB capability has changed. • **GRChange**—The GR capability has changed. • **BFDDown**—The interface is shut down by BFD. • **BadLSReq**—The interface receives BadLSReq events. • **SeqMismatch**—The interface receives SeqNumberMismatch events. • **1-Way**—The interface receives 1-Way events. • **LocalNoLSA**—The requested LSA does not exist. • **SameLSAReq**—The received LSA is in the local request queue. • **OldLSAReq**—The received LSA has a larger aging time than the requested LSA in the local request queue. • **DdTimerOut**—Receives a DD packet after the hello timer expires. • **EAChange**—The External Attribute bit has changed. • **RecvNoDupPkt**—Receives a non-duplicate DD packet in loading or full status. • **EbitChange**—The E bit has changed. • **MSbitChange**—The MS bit has changed. • **IbitChange**—The I bit has changed. • **MSeqNumError**—The primary router receives an unexpected serial number from the secondary router. • **SSeqNumError**—The secondary router receives an unexpected serial number from the primary router. • **RecvOpqIntf**—A DD packet that contains a type 9 LSA is received when the opaque LSA reception and advertisement capability is disabled. • **RecvOpqArea**—A DD packet that contains a type 10 LSA is received when the opaque LSA reception and advertisement capability is disabled. • **RecvOpqAs**—A DD packet that contains a type 11 LSA is received when the opaque LSA reception and advertisement capability is disabled. • **RecvNSSA**—A DD packet that contains a type 7 LSA is received in a non-NSSA area. • **InvalidLSA**—A DD packet that contains an invalid LSA is received. • **RecvASE**—A DD packet that contains a type 5 LSA is received on a virtual link or in a stub area.

Related commands

`reset ospf event-log`

display ospf event-log hello

Use **`display ospf event-log hello`** to display OSPF log information about received or sent hello packets.

NOTE:

This command is supported only in Release 6342 and later.

Syntax

`display ospf` [*`process-id`*] **`event-log hello`** { **`received`** [**`abnormal`** | **`dropped`**] | **`sent`** [**`abnormal`** | **`failed`**] } [*`neighbor-id`*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays OSPF log information for all processes.

received: Specifies log information for received hello packets.

sent: Specifies log information for sent hello packets.

abnormal: Specifies log information for abnormal hello packets received or sent at intervals greater than or equal to 1.5 times the hello interval.

dropped: Specifies log information for received hello packets that were dropped.

failed: Specifies log information for hello packets that failed to be sent.

neighbor-id: Specifies a neighbor by its ID. If you do not specify this argument, the command displays hello packet log information for all neighbors.

Examples

Display log information about sent hello packets.

```
<Sysname> display ospf event-log hello sent

         OSPF Process 1 with Router ID 5.5.5.5
                 Hello Log

Interface: Vlan10
Neighbor address: 10.1.1.2, NbrID: 1.0.0.2
First 4 hello packets sent:
  2019-09-05 20:10:10:121, failed, errno: 132
  2019-09-05 20:10:20:121, succeeded
  2019-09-05 20:10:30:121, succeeded
  2019-09-05 20:10:40:121, succeeded
Last 4 hello packets sent before Full->Down at 2019-09-06 14:52:10:121
  2019-09-06 14:51:40:021, succeeded
  2019-09-06 14:51:50:021, succeeded
  2019-09-06 14:52:00:021, failed, errno: 132
  2019-09-06 14:52:10:010, failed, errno: 132

Interface: Vlan10
Neighbor address: 10.1.1.2, NbrID: 1.0.0.2
First 4 hello packets sent:
  2019-09-05 20:10:10:121, failed, errno: 132
  2019-09-05 20:10:20:121, succeeded
  2019-09-05 20:10:30:121, succeeded
  2019-09-05 20:10:40:121, succeeded
Last 4 hello packets sent before Full->Init at 2019-09-06 11:16:20:171
  2019-09-06 11:15:20:121, succeeded
  2019-09-06 11:15:30:121, succeeded
  2019-09-06 11:15:40:121, succeeded
```

```
  2019-09-06 11:15:50:121, succeeded
```

Table 9 Command output

Field	Description
Interface	Interface that sent the hello packets.
Neighbor address	IP address of the neighbor.
NbrID	Router ID of the neighbor.
First 4 hello packets sent	Time and result (**succeeded** or **failed**) for sending the first four hello packets. For a packet failed to be sent, an error code is displayed in the **errno** field.
Last 4 hello packets sent before Full->Down at 2018-01-06 14:52:10:121	Time and result (**succeeded** or **failed**) for sending the last four hello packets before neighbor state change. For a packet failed to be sent, an error code is displayed in the **errno** field.

Display log information about the hello packets that failed to be sent.

```
<Sysname> display ospf event-log hello sent failed

          OSPF Process 1 with Router ID 5.5.5.5
                  Hello Log

Date: 2019-09-06 Time: 14:51:20:121 Interface: Vlan10
Destination address: 224.0.0.5, sent failed, errno: 132

Date: 2019-09-06 Time: 11:20:20:116 Interface: Vlan11
Destination address: 10.1.1.2, sent failed, errno: 132
```

Table 10 Command output

Field	Description
Date	Date for the hello packet sending failure, in the format of YYYY-MM-DD. YYYY represents the year, MM represents the month, and DD represents the day.
Time	Time for the hello packet sending failure, in the format of hh:mm:ss:xxx. hh represents the hours, mm represents the minutes, and ss represents the seconds, and xxx represents the milliseconds.
Interface	Interface that sent the hello packet.
Destination address	Destination IP address of the hello packet.
error	Error code for the hello packet sending failure.

Display log information about the abnormal hello packets sent.

```
<Sysname> display ospf event-log hello sent abnormal

          OSPF Process 1 with Router ID 5.5.5.5
                  Hello Log

Date: 2019-09-06 Time: 11:21:12:121 Interface: Vlan11
Destination address: 224.0.0.5, last one sent: 2019-09-06 11:20:51:916
```

```
Date: 2019-09-06 Time: 11:56:21:312 Interface: Vlan11
Destination address: 10.1.1.2, last one sent: 2019-09-06 11:56:02:691
```

Table 11 Command output

Field	Description
Date	Date for sending the abnormal hello packet, in the format of YYYY-MM-DD. YYYY represents the year, MM represents the month, and DD represents the day.
Time	Time for sending the abnormal hello packet, in the format of hh:mm:ss:xxx. hh represents the hours, mm represents the minutes, and ss represents the seconds, and xxx represents the milliseconds.
Interface	Interface that sent the abnormal hello packet.
Destination address	Destination IP address of the abnormal hello packet.
last one sent	Time for sending the last hello packet before sending the abnormal hello packet.

Display log information about received hello packets.

```
<Sysname> display ospf event-log hello received

         OSPF Process 1 with Router ID 5.5.5.5
                 Hello Log

Interface: Vlan10
Neighbor address: 10.1.1.2, NbrID: 1.0.0.2
First 4 hello packets received:
  2019-09-05 20:11:10:121
  2019-09-05 20:11:20:121
  2019-09-05 20:11:30:121
  2019-09-05 20:11:40:121
Last 4 hello packets received before Exchange->Down at 2019-09-06 14:52:10:121
  2019-09-06 14:51:10:121
  2019-09-06 14:51:20:121
  2019-09-06 14:51:30:121
  2019-09-06 14:51:40:121

Interface: Vlan10
Neighbor address: 10.1.1.1, NbrID: 1.0.0.1
First 4 hello packets received:
  2019-09-06 19:11:15:121
  2019-09-06 19:11:25:121
  2019-09-06 19:11:35:121
  2019-09-06 19:11:45:121
Last 4 hello packets received before Full->Init at 2019-09-06 21:16:20:171
  2019-09-06 21:15:45:121
  2019-09-06 21:15:55:121
  2019-09-06 21:16:05:121
  2019-09-06 21:16:15:121
```

Table 12 Command output

Field	Description
Interface	Interface that received the hello packets.
Neighbor address	IP address of the neighbor.
NbrID	Router ID of the neighbor.
First 4 hello packets received	Time for receiving the first four hello packets.
Last 4 hello packets received before Full->Init at 2019-09-06 21:16:20:171	Time for receiving the last four hello packets before neighbor state change, in the format of YYYY-MM-DD hh:mm:ss:xxx. YYYY represents the year, MM represents the month, and DD represents the day. hh represents the hours, mm represents the minutes, and ss represents the seconds, and xxx represents the milliseconds.

Display log information about the received hello packets that were dropped.

```
<Sysname> display ospf event-log hello received dropped

         OSPF Process 1 with Router ID 5.5.5.5
                 Hello Log

Date: 2019-09-06 Time: 14:51:22:791 Interface: Vlan10
Source address: 10.1.1.1, NbrID: 1.0.0.1, area: 0.0.0.1
Drop reason: Hello-time mismatch

Date: 2019-09-06 Time: 14:51:20:121 Interface: Vlan10
Source address: 10.1.1.2, NbrID: 1.0.0.2, area: 0.0.0.1
Drop reason: NP-bit mismatch
```

Table 13 Command output

Field	Description
Date	Date for dropping the received hello packet, in the format of YYYY-MM-DD. YYYY represents the year, MM represents the month, and DD represents the day.
Time	Time for dropping the received hello packet, in the format of hh:mm:ss:xxx. hh represents the hours, mm represents the minutes, and ss represents the seconds, and xxx represents the milliseconds.
Interface	Interface that received the hello packet.
Source address	Source IP address of the received hello packet.
NbrID	Router ID of the neighbor.
area	Area to which the neighbor interface belongs.
Drop reason	Reason for dropping the hello packet: • **Area under reset**—The area is in the reset progress. • **Router ID conflict**—Route ID conflict. • **Area mismatch**—Area ID mismatch. • **Unknown virtual router**—The hello packet is from an unknown virtual link. • **Authentication failure**—Authentication check failure. • **Peer address check**—Neighbor address check failure.

	• **Not DR or BDR**—The destination IP address of the hello packet is 224.0.0.6, but the interface is not a DR or BDR. • **Unknown unicast peer**—The hello packet is from an unknown unicast neighbor. • **Option mismatch**—Option mismatch. • **Netmask mismatch**—Subnet mask mismatch. • **Address mismatch**—Address range mismatch. • **Hello-time mismatch**—Hello timer mismatch. • **Dead-time mismatch**—Dead timer mismatch. • **Peer changed**—The source IP address or router ID has changed.

Display log information about the abnormal hello packets received.

```
<Sysname> display ospf event-log hello received abnormal

         OSPF Process 1 with Router ID 5.5.5.5
                 Hello Log

Date: 2019-09-06 Time: 10:12:22:121 Interface: Vlan10
Source address: 10.1.1.2, NbrID: 1.0.0.2, area: 0.0.0.1
Last one received: 2019-09-06 10:12:04:212

Date: 2019-09-06 Time: 14:51:20:121 Interface: Vlan10
Source address: 10.1.1.2, NbrID: 1.0.0.2, area: 0.0.0.1
Last one received: 2019-09-06 14:51:05:113
```

Table 14 Command output

Field	Description
Date&Tme	Date for receiving the abnormal hello packet, in the format of YYYY-MM-DD. YYYY represents the year, MM represents the month, and DD represents the day.
Time	Time for receiving the abnormal hello packet, in the format of hh:mm:ss:xxx. hh represents the hours, mm represents the minutes, and ss represents the seconds, and xxx represents the milliseconds.
Interface	Interface that received the abnormal hello packet.
Source address	Source IP address of the received abnormal hello packet.
NbrID	Router ID of the neighbor.
area	Area to which the neighbor interface belongs.
Last one received	Time for receiving the last hello packet before receiving the abnormal hello packet.

Related commands

`reset ospf event-log hello`

display ospf fast-reroute lfa-candidate

Use **`display ospf fast-reroute lfa-candidate`** to display OSPF FRR backup next hop information.

Syntax

display ospf [*process-id*] [**area** *area-id*] **fast-reroute lfa-candidate**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays FRR backup next hop information for all processes.

area *area-id*: Specifies an OSPF area by its ID. The area ID is an IP address or a decimal integer in the range of 0 to 4294967295 that is translated into the IP address format. If you do not specify this option, the command displays FRR backup next hop information for all OSPF areas.

Examples

Display OSPF FRR backup next hop information.

```
<Sysname> display ospf 1 area 0 fast-reroute lfa-candidate

          OSPF Process 1 with Router ID 2.2.2.2
                  LFA Candidate List

                Topology base (MTID 0)

 Area: 0.0.0.0
 Candidate nexthop count: 2
 NextHop          IntIP            Interface
 10.0.1.1         10.0.1.2         Vlan10
 10.0.11.1        10.0.11.2        Vlan20
```

Table 15 Command output

Field	Description
Topology	Topology name. The topology name for base topology is **base**.
MTID	Topology ID. The value of 0 indicates the base topology.
Area	Area to which the backup next hops belong.
Candidate nexthop count	Number of backup next hops.
NextHop	Backup next hop address.
IntIP	IP address of the output interface.
Interface	Output interface.

display ospf graceful-restart

Use **display ospf graceful-restart** to display GR information.

Syntax

display ospf [*process-id*] **graceful-restart** [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays GR information for all processes.

verbose: Displays detailed GR information. If you do not specify this keyword, the command displays brief GR information.

Examples

Display detailed GR information.

```
<Sysname> display ospf graceful-restart verbose

          OSPF Process 1 with Router ID 1.1.1.1
              Graceful Restart information

Graceful Restart capability     : Enable(IETF)
Graceful Restart support        : Planned and unplanned,Partial
Helper capability               : Enable(IETF)
Helper support                  : Planned and unplanned(IETF),Strict LSA check
Current GR state                : Normal
Graceful Restart period         : 40 seconds
Number of neighbors under Helper: 0
Number of restarting neighbors  : 0
Last exit reason:
  Restarter  : None
  Helper     : None

Area: 0.0.0.0
Authtype: None Area flag: Normal
Area up Interface count: 2

Interface: 40.4.0.1 (Vlan-interface40)
Restarter state: Normal  State: P-2-P     Type: PTP
Last exit reason:
  Restarter  : None
  Helper     : None
Neighbor count of this interface: 1
Number of neighbors under Helper: 0
Neighbor        IP address      GR state     Last Helper exit reason
3.3.3.3         40.4.0.3        Normal       None

Virtual-link Neighbor-ID  -> 4.4.4.4, Neighbor-State: Full
Restarter state: Normal
Interface: 20.2.0.1 (Vlink)
```

```
Transit Area: 0.0.0.1
Last exit reason:
  Restarter  : None
  Helper     : None
Neighbor        IP address      GR state     Last Helper exit reason
4.4.4.4         20.2.0.4        Normal       Reset neighbor
```

Table 16 Command output

Field	Description
OSPF Process 1 with Router ID 1.1.1.1 Graceful Restart information	GR information for OSPF process 1 with router ID 1.1.1.1.
Graceful Restart capability	Whether GR is enabled: • **Enable(IETF)**—IETF GR is enabled. • **Enable(Nonstandard)**—Non-IETF GR is enabled. • **Disable**—GR is disabled.
Graceful Restart support	GR modes that the process supports (displayed only when GR is enabled): • **Planned and unplanned**—Supports both planned and unplanned GR. • **Planned only**—Supports only planned GR. • **Partial**—Supports partial GR. • **Global**—Supports global GR.
Helper capability	Helper capability that the process supports: • **Enable(IETF)**—Supports IETF GR helper capability. • **Enable(Nonstandard)**—Supports non-IETF GR helper capability. • **Enable(IETF and nonstandard)**—Supports both IETF GR helper capability and non-IETF GR helper capability. • **Disable**—Does not support GR helper capability.
Helper support	Policies that the helper supports (displayed only when GR helper is enabled): • **Strict lsa check**—The helper supports strict LSA checking. • **Planned and unplanned**—The helper supports planned and unplanned GR. • **Planned only**—The helper supports only planned GR.
Current GR state	GR state: • **Normal**—GR is not in progress or has completed. • **Under GR**—GR is in process. • **Under Helper**—The process is acting as GR helper.
Last exit reason	Last exit reason: • **Restarter**—Reason that the restarter exited most recently. • **Helper**—Reason that the helper exited most recently.
Area	Area ID in IP address format.
Authtype	Authentication type of the area: • **None**—No authentication. • **Simple**—Simple authentication. • **MD5**—MD5 authentication.

Field	Description
Area flag	Type of the area: • Normal. • Stub. • StubNoSummary (totally stub area). • NSSA. • NSSANoSummary (totally NSSA area).
Area up Interface count	Number of up interfaces in the area.
Interface	Interface in the area.
Restarter state	Restarter state on the interface.
State	Interface state.
Type	Interface network type.
Neighbor count of this interface	Neighbors of an interface.
Neighbor	Neighbor router ID.
IP address	Neighbor IP address.
GR state	Neighbor GR state: • **Normal**—GR is not in progress or has completed. • **Under GR**—GR is in process. • **Under Helper**—The process is acting as GR helper.
Last Helper exit reason	Reason that the helper exited most recently.
Virtual-link Neighbor-ID	Router ID of the virtual link's neighbor.
Neighbor-State	Neighbor state: Down, Init, 2-Way, ExStart, Exchange, Loading, and Full.
Interface	Output interface of the virtual link.

display ospf interface

Use **`display ospf interface`** to display OSPF interface information.

Syntax

`display ospf` [*`process-id`*] **`interface`** [*`interface-type interface-number`* | **`verbose`**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

`process-id`: Specifies an OSPF process ID in the range of 1 to 65535. If you do not specify this argument, the command displays the OSPF interface information for all OSPF processes.

`interface-type interface-number`: Specifies an interface by its type and number.

`verbose`: Displays detailed OSPF information for all interfaces.

Usage guidelines

If you do not specify the *interface-type interface-number* argument or the **verbose** keyword, this command displays OSPF brief information for all interfaces.

Examples

Display all OSPF interface brief information.

```
<Sysname> display ospf interface

          OSPF Process 1 with Router ID 192.168.1.1
                  Interfaces

 Area: 0.0.0.0
 IP Address      Type         State    Cost  Pri   DR              BDR
 192.168.1.1     PTP          P-2-P    1562  1     0.0.0.0         0.0.0.0

 Area: 0.0.0.1
 IP Address      Type         State    Cost  Pri   DR              BDR
 172.16.0.1      Broadcast    DR       1     1     172.16.0.1      0.0.0.0
```

Table 17 Command output

Field	Description
Area	Area ID of the interface.
IP Address	Interface IP address (regardless of whether TE is enabled or not).
Type	Interface network type: PTP (P2P), PTMP (P2MP), Broadcast, or NBMA.
State	Interface state: • **Down**—No protocol traffic can be sent or received on the interface. • **Loopback**—The interface is in loopback state and it cannot forward traffic. • **Waiting**—The interface starts sending and receiving Hello packets. The router is trying to determine the identity of the (Backup) designated router for the network. • **P-2-P**—The interface will send Hello packets at the hello interval, and try to establish an adjacency with the neighbor. • **DR**—The router is the designated router on the network. • **BDR**—The router is the backup designated router on the network. • **DROther**—The router is a DR Other router on the attached network.
Cost	Interface cost.
Pri	Router priority.
DR	DR on the interface's network segment.
BDR	BDR on the interface's network segment.

Display detailed information about VLAN-interface 10.

```
<Sysname> display ospf interface vlan-interface 10

          OSPF Process 1 with Router ID 192.168.1.1
                  Interfaces

 Area: 0.0.0.0
```

```
Interface: 172.16.0.1 (Vlan-interface10)
Cost: 1       State: DR        Type: Broadcast    MTU: 1500
Priority: 1
Designated router: 172.16.0.1
Backup designated router: 0.0.0.0
Timers: Hello 10, Dead 40, Poll  40, Retransmit 5, Transmit Delay 1
FRR backup: Enabled
Primary path detection mode: BFD ctrl
Enabled by interface configuration (including secondary IP addresses)
BFD: echo
MD5 authentication enabled.
   The last key is 3.
   The rollover is in progress, 2 neighbor(s) left.
LDP state: No-LDP
LDP sync state: Achieved
Packet size: 1000
```

Table 18 Command output

Field	Description
Interface	Information about the interface, such as the IP address.
Timers	OSPF timers (in seconds): **Hello**, **Dead**, **Poll**, and **Retransmit**.
Transmit Delay	LSA transmission delay on the interface, in seconds.
FRR backup	Whether LFA calculation is enabled on an interface.
Primary path detection mode	Primary link detection mode: • **BFD ctrl**—BFD control packet mode. • **BFD echo**—BFD echo packet mode.
Enabled by interface configuration (including secondary IP addresses)	OSPF is enabled on the interface (including secondary IP addresses).
BFD	BFD session mode enabled on the interface: • **ctrl**—BFD control packet mode. • **echo**—BFD echo packet mode.
Simple authentication enabled	Simple authentication is enabled.
MD5 authentication enabled	MD5/HMAC-MD5 authentication is enabled.
The last key is *xx*	The most recent MD5/HMAC-MD5 authentication key ID is *xx*.
The rollover is in progress, *xx* neighbor(s) left.	Key rollover for MD5/HMAC-MD5 authentication is in progress. The number of neighbors that have not completed rollover is *xx*.
LDP state	LDP state: • **Init**—Initialization state. LDP has not been delivered. • **No-LDP**—LDP is not configured. • **Not ready**—LDP sessions have not been established. • **Ready**—LDP sessions have been established.

Field	Description
LDP sync state	LDP IGP synchronization state: • **Init**—Initialization state. • **Achieved**—LDP has been synchronized. • **Max cost**—OSPF advertises the maximum cost in LSAs.
Packet size	Maximum length of OSPF packets that can be sent by the interface.

display ospf interface hello

Use **display ospf interface hello** to display information about hello packets sent by OSPF interfaces.

NOTE:

This command is supported only in Release 6342 and later.

Syntax

display ospf [*process-id*] **interface** [*interface-type interface-number*] **hello**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPF process ID in the range of 1 to 65535. If you do not specify this argument, the command displays hello packet information for all OSPF processes.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify this argument, the command displays information about the hello packets sent by all OSPF interfaces.

Usage guidelines

This command displays information for only the hello packets sent in multicast.

Examples

Display hello packet information for all OSPF interfaces.

```
<Sysname> display ospf interface hello

          OSPF Process 1 with Router ID 192.168.1.1
                 Interfaces

 Area: 0.0.0.0

 Interface: 172.16.0.1 (Vlan-interface10)
 First 4 hello packets sent:
   2019-09-05 11:05:10:121, succeeded
   2019-09-05 11:05:20:121, succeeded
```

```
  2019-09-05 11:05:30:121, succeeded
  2019-09-05 11:05:40:121, succeeded
Last 4 hello packets sent:
  2019-09-06 11:15:10:121, succeeded
  2019-09-06 11:15:20:121, succeeded
  2019-09-06 11:15:30:121, succeeded
  2019-09-06 11:15:40:121, succeeded
```

Table 19 Command output

Field	Description
Area	Area to which the interface belongs.
Interface	IP address of the interface.
First 4 hello packets sent	Time and result (**succeeded** or **failed**) for sending the first four hello packets.
Last 4 hello packets sent	Time and result (**succeeded** or **failed**) for sending the last four hello packets when the command is executed.

display ospf lsdb

Use **display ospf lsdb** to display OSPF LSDB information.

Syntax

display ospf [*process-id*] **lsdb** [**brief** | **originate-router** *advertising-router-id* | **self-originate**]

display ospf [*process-id*] **lsdb** { **ase** | **opaque-as** } [*link-state-id*] [**originate-router** *advertising-router-id* | **self-originate**]

display ospf [*process-id*] **lsdb** { **asbr** | **network** | **nssa** | **opaque-area** | **opaque-link** | **router** | **summary** } [*link-state-id*] [**originate-router** *advertising-router-id* | **self-originate**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays LSDB information for all OSPF processes.

area *area-id*: Specifies an OSPF area by its ID. The area ID is an IP address or a decimal integer in the range of 0 to 4294967295 that is translated into the IP address format. If you do not specify this option, the command displays LSDB information for all OSPF areas.

brief: Displays brief LSDB information.

asbr: Displays Type-4 LSA (ASBR Summary LSA) information in the LSDB.

ase: Displays Type-5 LSA (AS External LSA) information in the LSDB.

network: Displays Type-2 LSA (Network LSA) information in the LSDB.

nssa: Displays Type-7 LSA (NSSA External LSA) information in the LSDB.

opaque-area: Displays Type-10 LSA (Opaque-area LSA) information in the LSDB.

opaque-as: Displays Type-11 LSA (Opaque-AS LSA) information in the LSDB.

opaque-link: Displays Type-9 LSA (Opaque-link LSA) information in the LSDB.

router: Displays Type-1 LSA (Router LSA) information in the LSDB.

summary: Displays Type-3 LSA (Network Summary LSA) information in the LSDB.

link-state-id: Specifies a link state ID in the IP address format.

originate-router *advertising-router-id*: Specifies an advertising router by its ID.

self-originate: Displays information about self-originated LSAs.

Examples

Display OSPF LSDB information.

```
<Sysname> display ospf lsdb
         OSPF Process 1 with Router ID 192.168.0.1
                 Link State Database

                         Area: 0.0.0.0
 Type      LinkState ID    AdvRouter          Age  Len   Sequence   Metric
 Router    192.168.0.2     192.168.0.2        474  36    80000004   0
 Router    192.168.0.1     192.168.0.1        21   36    80000009   0
 Network   192.168.0.1     192.168.0.1        321  32    80000003   0
 Sum-Net   192.168.1.0     192.168.0.1        321  28    80000002   1
 Sum-Net   192.168.2.0     192.168.0.2        474  28    80000002   1
                         Area: 0.0.0.1
 Type      LinkState ID    AdvRouter          Age  Len   Sequence   Metric
 Router    192.168.0.1     192.168.0.1        21   36    80000005   0
 Sum-Net   192.168.2.0     192.168.0.1        321  28    80000002   2
 Sum-Net   192.168.0.0     192.168.0.1        321  28    80000002   1
                         Type 9 Opaque (Link-Local Scope) Database
 Flags: * -Vlink interface LSA
 Type      LinkState ID    AdvRouter          Age  Len   Sequence   Interfaces
*Opq-Link  3.0.0.0         7.2.2.1            8    14    80000001   10.1.1.2
*Opq-Link  3.0.0.0         7.2.2.2            8    14    80000001   20.1.1.2
```

Table 20 Command output

Field	Description
Area	LSDB information for the area.
Type	LSA type.
LinkState ID	Link state ID.
AdvRouter	Advertising router.
Age	Age of the LSA.
Len	Length of the LSA.
Sequence	Sequence number of the LSA.
Metric	Cost of the LSA.

Field	Description
*Opq-Link	Opaque LSA generated by a virtual link.

Display Type-2 LSA (Network LSA) information in the LSDB.

```
<Sysname> display ospf 1 lsdb network

          OSPF Process 1 with Router ID 192.168.1.1
                  Link State Database

                          Area: 0.0.0.0

    Type      : Network
    LS ID     : 192.168.0.2
    Adv Rtr   : 192.168.2.1
    LS age    : 922
    Len       : 32
    Options   :  E
    Seq#      : 80000003
    Checksum    : 0x8d1b
    Net mask  : 255.255.255.0
       Attached router    192.168.1.1
       Attached router    192.168.2.1

                          Area: 0.0.0.1

    Type      : Network
    LS ID     : 192.168.1.2
    Adv Rtr   : 192.168.1.2
    LS age    : 782
    Len       : 32
    Options   :  NP
    Seq#      : 80000003
    Checksum    : 0x2a77
    Net mask  : 255.255.255.0
       Attached router    192.168.1.1
       Attached router    192.168.1.2
```

Table 21 Command output

Field	Description
Type	LSA type.
LS ID	DR IP address.
Adv Rtr	Router that advertised the LSA.
LS age	LSA age time.
Len	LSA length.

Field	Description
Options	LSA options: • **O**—Opaque LSA advertisement capability. • **E**—AS External LSA reception capability. • **EA**—External extended LSA reception capability. • **DC**—On-demand link support. • **N**—NSSA external LSA support. • **P**—Capability of an NSSA ABR to translate Type-7 LSAs into Type-5 LSAs.
Seq#	LSA sequence number.
Checksum	LSA checksum.
Net mask	Network mask.
Attached router	ID of the router that established adjacency with the DR, and ID of the DR itself.

display ospf nexthop

Use **display ospf nexthop** to display OSPF next hop information.

Syntax

display ospf [*process-id*] **nexthop**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays next hop information for all OSPF processes.

Examples

Display OSPF next hop information.

```
<Sysname> display ospf nexthop

          OSPF Process 1 with Router ID 1.1.1.2
                  Neighbor Nexthop Information

 NbrID           Nexthop         Interface               RefCount   Status
 192.168.12.1    0.0.0.0         Vlan10                  4          Valid
 192.168.12.2    192.168.12.2    Vlan10                  3          Valid
 192.168.12.1    0.0.0.0         Loop100                 1          Valid
```

Table 22 Command output

Field	Description
NbrID	Neighbor router ID.

Field	Description
Nexthop	Next hop address.
Interface	Output interface.
RefCount	Reference count (routes that use the next hop).
Status	Next hop status: valid or invalid.

display ospf non-stop-routing status

Use **display ospf non-stop-routing status** to display OSPF NSR information.

Syntax

display ospf [*process-id*] **non-stop-routing status**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays OSPF NSR information for all OSPF processes.

Examples

Display OSPF NSR information.

```
<Sysname> display ospf non-stop-routing status

                  OSPF Process 1 with Router ID 192.168.33.12
                        Non Stop Routing information

Non Stop Routing capability : Enabled
Upgrade phase : Normal
```

Table 23 Command output

Field	Description
Non Stop Routing capability	NSR status: enabled or disabled.
Upgrade phase	Upgrade phase: • **Prepare**—Upgrade preparation phase. • **Restore Smooth**—Upgrade phase. • **Preroute**—Route pre-calculation phase. • **Calculating**—Route calculation phase. • **Redisting**—Route redistribution phase. • **Original and age**—LSA generation and aging phase. • **Normal**—Normal status.

display ospf peer

Use **display ospf peer** to display information about OSPF neighbors.

Syntax

display ospf [*process-id*] **peer** [**hello** | **verbose**] [*interface-type interface-number*] [*neighbor-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPF process by ID in the range of 1 to 65535. If you do not specify this argument, the command displays OSPF neighbor information for all OSPF processes.

hello: Displays information about the hello packets sent to and received from neighbor routers. In scenarios where hello packets are sent in multicast, the command displays information only about the hello packets received from neighbor routers.

verbose: Displays detailed neighbor information. If you do not specify this keyword, the command displays brief OSPF neighbor information.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify this argument, the command displays neighbor information for all interfaces.

neighbor-id: Specifies a neighbor router ID. If you do not specify this argument, the command displays all neighbor information.

Examples

Display detailed OSPF neighbor information.

```
<Sysname> display ospf peer verbose

          OSPF Process 1 with Router ID 1.1.1.1
                  Neighbors

 Area 0.0.0.0 interface 1.1.1.1(Vlan-interface100)'s neighbors
 Router ID: 1.1.1.2          Address: 1.1.1.2          GR state: Normal
   State: Full  Mode: Nbr is master  Priority: 1
   DR: 1.1.1.2  BDR: 1.1.1.1  MTU: 0
   Options is 0x02 (-|-|-|-|-|-|E|-)
   Dead timer due in 33  sec
   Neighbor is up for 02:03:35
   Authentication sequence: [ 0 ]
   Neighbor state change count: 6
   BFD status: Disabled


 Last Neighbor Down Event:
 Router ID: 22.22.22.22
 Local Address: 11.11.11.11
```

```
Remote Address: 22.22.22.22
Time: Apr  9 03:18:19 2014
Reason: Ospf_ifachange
```

Table 24 Command output

Field	Description
Area *areaID* interface *IPAddress*(*InterfaceName*)'s neighbors	Neighbor information for the interface in the specified area: • **areaID**—Area to which the neighbor belongs. • **IPAddress**—Interface IP address. • **InterfaceName**—Interface name.
Router ID	Neighbor router ID.
Address	Neighbor router address.
GR state	GR state: • Normal. • Restarter. • Complete. • Helper.
State	Neighbor state: • **Down**—Initial state of a neighbor conversation. • **Init**—The router has received a Hello packet from the neighbor. However, the router has not established bidirectional communication with the neighbor. The router did not appear in the neighbor's hello packet. • **Attempt**—Available only in an NBMA network. In this state, the OSPF router has not received any information from a neighbor for a period. The router can send Hello packets at a longer interval to keep the neighbor relationship. • **2-Way**—Communication between the two routers is bidirectional. The local router appears in the neighbor's Hello packet. • **Exstart**—The goal of this state is to decide which router is the master, and to decide upon the initial Database Description (DD) sequence number. • **Exchange**—The router is sending DD packets to the neighbor, describing its entire link-state database. • **Loading**—The router sends LSRs packets to the neighbor, requesting more recent LSAs. • **Full**—The neighboring routers are fully adjacent.
Mode	Neighbor mode for LSDB synchronization.
Priority	Neighboring router priority.
DR	DR on the interface's network segment.
BDR	BDR on the interface's network segment.
MTU	Interface MTU.

Field	Description
Options	LSA options: • **O**—Opaque LSA advertisement capability. • **E**—AS External LSA reception capability. • **EA**—External extended LSA reception capability. • **DC**—On-demand link support. • **N**—NSSA external LSA support. • **P**—Capability of an NSSA ABR to translate Type-7 LSAs into Type-5 LSAs.
Dead timer due in 33 sec	This dead timer will expire in 33 seconds.
Neighbor is up for 02:03:35	The neighbor has been up for 02:03:35.
Authentication sequence	Authentication sequence number.
Neighbor state change count	Count of neighbor state changes.
BFD status	BFD status: • Disabled. • Enabled (Control mode). • Enabled (Echo mode).
Last Neighbor Down Event	The most recent neighbor down event.
Time	Time when the neighbor went down.
Reason	Reason for the neighbor down event.

Display brief OSPF neighbor information.

```
<Sysname> display ospf peer

          OSPF Process 1 with Router ID 1.1.1.1
               Neighbor Brief Information

 Area: 0.0.0.0
 Router ID       Address         Pri Dead-Time  State             Interface
 1.1.1.2         1.1.1.2         1   40         Full/DR           Vlan10
```

Table 25 Command output

Field	Description
Area	Neighbor area.
Router ID	Neighbor router ID.
Address	Neighbor interface address.
Pri	Neighboring router priority.
Dead-Time	Dead interval remained.
Interface	Interface connected to the neighbor.
State	Neighbor state: Down, Init, Attempt, 2-Way, Exstart, Exchange, Loading, or Full.

Display detailed information about the hello packets sent to and received from neighbor routers.

```
<Sysname> display ospf peer hello
```

```
          OSPF Process 1 with Router ID 1.1.1.1
                  Neighbors

 Area 0.0.0.0 interface 1.1.1.1(Vlan-interface10)'s neighbors
 Router ID: 1.1.1.2          Address: 1.1.1.2
 First 4 hello packets received:
   2019-09-06 09:12:10:121
   2019-09-06 09:12:20:121
   2019-09-06 09:12:30:121
   2019-09-06 09:12:40:121
 Last 4 hello packets received:
   2019-09-06 11:15:10:121
   2019-09-06 11:15:20:121
   2019-09-06 11:15:30:121
   2019-09-06 11:15:40:121
 First 4 hello packets sent:
   2019-09-06 09:12:12:121, failed, errno:132
   2019-09-06 09:12:22:121, succeeded
   2019-09-06 09:12:32:121, succeeded
   2019-09-06 09:12:42:121, succeeded
 Last 4 hello packets sent:
   2019-09-06 11:15:12:121, succeeded
   2019-09-06 11:15:22:121, succeeded
   2019-09-06 11:15:32:121, failed, errno:132
   2019-09-06 11:15:42:121, failed, errno:132
```

Table 26 Command output

Field	Description
Router ID	Router ID of the neighbor.
Address	IP address of the neighbor interface.
First 4 hello packets received	Time for receiving the first four hello packets from neighbors.
Last 4 hello packets received	Time for receiving the last four hello packets from neighbors.
First 4 hello packets sent	Time and result (**succeeded** or **failed**) for sending the first four hello packets to neighbors. For a packet failed to be sent, an error code is displayed in the **errno** field. This field is not displayed in scenarios where hello packets are sent in multicast.
Last 4 hello packets sent	Time and result (**succeeded** or **failed**) for sending the last four hello packets to neighbors when the command is executed. For a packet failed to be sent, an error code is displayed in the **errno** field. This field is not displayed in scenarios where hello packets are sent in multicast.

display ospf peer statistics

Use **display ospf peer statistics** to display OSPF neighbor statistics.

Syntax

display ospf [*process-id*] **peer statistics**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays OSPF neighbor statistics for all OSPF processes.

Examples

Display OSPF neighbor statistics.

```
<Sysname> display ospf peer statistics
          OSPF Process 1 with Router ID 10.3.1.1
                    Neighbor Statistics
  Area ID         Down Attempt Init 2-Way ExStart Exchange Loading Full Total
  0.0.0.0         0    0       0    0     0       0        0       1    1
  0.0.0.2         0    0       0    0     0       0        0       1    1
  Total           0    0       0    0     0       0        0       2    2
```

Table 27 Command output

Field	Description
Area ID	The state statistics for all the routers in the area to which the router belongs is displayed.
Down	Number of neighboring routers in Down state in the same area.
Attempt	Number of neighboring routers in Attempt state in the same area.
Init	Number of neighboring routers in Init state in the same area.
2-Way	Number of neighboring routers in 2-Way state in the same area.
ExStart	Number of neighboring routers in ExStart state in the same area.
Exchange	Number of neighboring routers in Exchange state in the same area.
Loading	Number of neighboring routers in Loading state in the same area.
Full	Number of neighboring routers in Full state in the same area.
Total	Total number of neighbors in the same state: Down, Attempt, Init, 2-Way, ExStart, Exchange, Loading, or Full.

display ospf request-queue

Use **display ospf request-queue** to display OSPF request queue information.

Syntax

display ospf [*process-id*] **request-queue** [*interface-type interface-number*] [*neighbor-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays the OSPF request queue information for all OSPF processes.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify this argument, the command displays the OSPF request queue information for all interfaces.

neighbor-id: Specifies a neighbor's router ID. If you do not specify this argument, the command displays the OSPF request queue information for all OSPF neighbors.

Examples

Display OSPF request queue information.

```
<Sysname> display ospf request-queue

          OSPF Process 100 with Router ID 192.168.1.59
                  Link State Request List

  The Router's Neighbor is Router ID 2.2.2.2         Address 10.1.1.2
  Interface 10.1.1.1         Area 0.0.0.0
  Request list:
       Type       LinkState ID      AdvRouter         Sequence   Age
       Router     2.2.2.2           1.1.1.1           80000004   1
       Network    192.168.0.1       1.1.1.1           80000003   1
       Sum-Net    192.168.1.0       1.1.1.1           80000002   2
```

Table 28 Command output

Field	Description
The Router's Neighbor is Router ID	Neighbor router ID.
Address	Neighbor interface IP address.
Interface	Local interface IP address.
Area	Area ID.
Request list	Request list information.
Type	LSA type.
LinkState ID	Link state ID.
AdvRouter	Advertising router.
Sequence	LSA sequence number.
Age	LSA age.

display ospf retrans-queue

Use **display ospf retrans-queue** to display retransmission queue information.

Syntax

display ospf [*process-id*] **retrans-queue** [*interface-type interface-number*] [*neighbor-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays retransmission queue information for all OSPF processes.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify this argument, the command displays retransmission queue information for all interfaces.

neighbor-id: Specifies a neighbor's router ID. If you do not specify this argument, the command displays retransmission queue information for all neighbors.

Examples

Display OSPF retransmission queue information.

```
<Sysname> display ospf retrans-queue

          OSPF Process 100 with Router ID 192.168.1.59
                  Link State Retransmission List

  The Router's Neighbor is Router ID 2.2.2.2         Address 10.1.1.2
  Interface 10.1.1.1         Area 0.0.0.0
  Retransmit list:
       Type       LinkState ID      AdvRouter         Sequence   Age
       Router     2.2.2.2           2.2.2.2           80000004   1
       Network    12.18.0.1         2.2.2.2           80000003   1
       Sum-Net    12.18.1.0         2.2.2.2           80000002   2
```

Table 29 Command output

Field	Description
The Router's Neighbor is Router ID	Neighbor router ID.
Address	Neighbor interface IP address.
Interface	Interface address of the router.
Area	Area ID.
Retransmit list	Retransmission list.
Type	LSA type.
LinkState ID	Link state ID.

Field	Description
AdvRouter	Advertising router.
Sequence	LSA sequence number.
Age	LSA age.

display ospf routing

Use **display ospf routing** to display OSPF routing information.

Syntax

display ospf [*process-id*] **routing** [*ip-address* { *mask-length* | *mask* }] [**interface** *interface-type interface-number*] [**nexthop** *nexthop-address*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays the routing information for all OSPF processes.

ip-address: Specifies a destination IP address.

mask-length: Specifies mask length in the range of 0 to 32.

mask: Specifies the mask in dotted decimal notation.

interface *interface-type interface-number*: Displays routes passing the specified output interface. If you do not specify this option, the command displays OSPF routing information for all interfaces.

nexthop *nexthop-address*: Displays routes passing the specified next hop. If you do not specify this option, the command displays all OSPF routing information.

verbose: Displays detailed OSPF routing information. If you do not specify this keyword, the command displays brief OSPF routing information.

Examples

Display OSPF routing information.

```
<Sysname> display ospf routing

          OSPF Process 1 with Router ID 192.168.1.2
                  Routing Table

                Topology base (MTID 0)

 Routing for network
 Destination        Cost  Type       NextHop         AdvRouter     Area
 192.168.1.0/24     1562  Stub       192.168.1.2     192.168.1.2   0.0.0.0
```

```
172.16.0.0/16      1563  Inter      192.168.1.1     192.168.1.1   0.0.0.0

Total nets: 2
Intra area: 1  Inter area: 1  ASE: 0  NSSA: 0
```

Table 30 Command output

Field	Description
Topology	Topology name. The topology name for base topology is **base**.
MTID	Topology ID. The value of 0 indicates the base topology.
Destination	Destination network.
Cost	Cost to destination.
Type	Route type: intra, transit, stub, inter, Type-1, and Type-2.
NextHop	Next hop address.
AdvRouter	Advertising router.
Area	Area ID.
Total nets	Total networks.
Intra area	Total intra-area routes.
Inter area	Total inter-area routes.
ASE	Total ASE routes.
NSSA	Total NSSA routes.

Display detailed OSPF routing information.

```
<Sysname> display ospf routing verbose

          OSPF Process 2 with Router ID 192.168.1.112
                   Routing Table

                Topology base (MTID 0)

 Routing for network

 Destination: 192.168.1.0/24
    Priority: Low                    Type: Stub
   AdvRouter: 192.168.1.2            Area: 0.0.0.0
  SubProtoID: 0x1               Preference: 10
     NextHop: 192.168.1.2        BkNextHop: N/A
      IfType: Broadcast           BkIfType: N/A
   Interface: Vlan100          BkInterface: N/A
       NibID: 0x1300000c            Status: Normal
        Cost: 1562

 Destination: 172.16.0.0/16
    Priority: Low                    Type: Inter
   AdvRouter: 192.168.1.1            Area: 0.0.0.0
  SubProtoID: 0x1               Preference: 10
```

```
    NextHop: 192.168.1.1        BkNextHop: N/A
     IfType: Broadcast           BkIfType: N/A
  Interface: Vlan101          BkInterface: N/A
      NibID: 0x1300000c            Status: Normal
       Cost: 1563

Total nets: 2
Intra area: 2  Inter area: 0  ASE: 0  NSSA: 0
```

Table 31 Command output

Field	Description
Topology	Topology name. The topology name for base topology is **base**.
MTID	Topology ID. The value of 0 indicates the base topology.
Priority	Prefix priority: critical, high, medium, and low.
Type	Route type: intra-area, transit, stub, inter-area, Type-1 external, and Type-2 external.
AdvRouter	Advertising router.
Area	Area ID.
SubProtoID	Sub protocol ID.
Preference	OSPF route preference.
NextHop	Primary next hop IP address.
BkNextHop	Backup next hop IP address.
IfType	Type of the network to which the primary next hop belongs.
BkIfType	Type of the network to which the backup next hop belongs.
Interface	Output interface.
BkInterface	Backup output interface.
NibID	Next hop ID.
Status	Route status: • **Local**—The route is on the local end and is not sent to the route management module. • **Invalid**—The next hop is invalid. • **Stale**—The next hop is stale. • **Normal**—The route is available. • **Delete**—The route is deleted. • **Host-Adv**—The route is a host route. • **Rely**—The route is a recursive route.
Cost	Cost to destination.

display ospf spf-tree

Use **display ospf spf-tree** to display SPF tree information.

Syntax

display ospf [*process-id*] [**area** *area-id*] **spf-tree** [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify a process, this command displays SPF tree information for all OSPF processes.

area *area-id*: Specifies an OSPF area by its ID. The area ID is an IP address or a decimal integer in the range of 0 to 4294967295 that is translated into the IP address format. If you do not specify an area, this command displays SPF tree information for all OSPF areas.

verbose: Displays detailed SPF tree information. If you do not specify this keyword, the command displays brief SPF tree information.

Examples

Display brief SPF tree information for Area 0 in OSPF process 1.

```
<Sysname> display ospf 1 area 0 spf-tree

          OSPF Process 1 with Router ID 100.0.0.4

        Flags: S-Node is on SPF tree       R-Node is directly reachable
               I-Node or Link is init      D-Node or Link is to be deleted
               P-Neighbor is parent        A-Node is in candidate list
               C-Neighbor is child         T-Node is tunnel destination
               H-Nexthop changed           N-Link is a new path
               V-Link is involved          G-Link is in change list

                Topology base (MTID 0)

                  Area: 0.0.0.0  Shortest Path Tree

 SpfNode         Type    Flag      SpfLink         Type   Cost  Flag
>192.168.119.130 Network S R
                                --->114.114.114.111 NET2RT 0     C
                                --->100.0.0.4       NET2RT 0     P
>114.114.114.111 Router  S
                                --->192.168.119.130 RT2NET 65535 P
>100.0.0.4       Router  S
                                --->192.168.119.130 RT2NET 10    C
```

Table 32 Command output

Field	Description
Topology	Topology name. The topology name for base topology is **base**.
MTID	Topology ID. The value of 0 indicates the base topology.

Field	Description
SpfNode	SPF node, represented by a router ID when the node type is **Router**, or the IP address of the DR when the node type is **Network**. Node flag: • **I**—The node is in initialization state. • **A**—The node is on the candidate list. • **S**—The node is on the SPF tree. • **R**—The node is directly connected to the root node. • **D**—The node is to be deleted. • **T**—The node is the tunnel destination. This flag is not supported in the current software version.
SpfLink	SPF link, representing the peer node. Link type: • **RT2RT**—Router to router. • **NET2RT**—Network to router. • **RT2NET**—Router to network. Link flag: • **I**—The link is in initialization state. • **P**—The peer is the parent node. • **C**—The peer is the child node. • **D**—The link is to be deleted. • **H**—The next hop is changed. • **V**—When the peer node is deleted or added, the peer node is not on the SPF tree or is deleted. • **N**—The link is newly added, and both end nodes are on the SPF tree. • **G**—The link is on the area change list.

Display detailed SPF tree information for Area 0 in OSPF process 1.

```
<Sysname> display ospf 1 area 0 spf-tree verbose

          OSPF Process 1 with Router ID 100.0.0.4

        Flags: S-Node is on SPF tree       R-Node is directly reachable
               I-Node or Link is init      D-Node or Link is to be deleted
               P-Neighbor is parent        A-Node is in candidate list
               C-Neighbor is child         T-Node is tunnel destination
               H-Nexthop changed           N-Link is a new path
               V-Link is involved          G-Link is in change list

                Topology base (MTID 0)

                  Area: 0.0.0.0  Shortest Path Tree

>LsId(192.168.119.130)
 AdvId    : 100.0.0.4       NodeType     : Network
 Mask     : 255.255.255.0   SPFLinkCnt   : 2
 Distance : 10
 VlinkData: 0.0.0.0         ParentLinkCnt: 1          NodeFlag: S R
```

```
NextHop  : 1
  192.168.119.130    Interface: Vlan100
BkNextHop: 1
  0.0.0.0            Interface: Vlan100
-->LinkId(114.114.114.111)
   AdvId   : 100.0.0.4       LinkType   : NET2RT
   LsId    : 192.168.119.130 LinkCost   : 0           NextHopCnt: 1
   LinkData: 0.0.0.0         LinkNewCost: 0           LinkFlag  : C
-->LinkId(100.0.0.4)
   AdvId   : 100.0.0.4       LinkType   : NET2RT
   LsId    : 192.168.119.130 LinkCost   : 0           NextHopCnt: 1
   LinkData: 0.0.0.0         LinkNewCost: 0           LinkFlag  : P
```

Table 33 Command output

Field	Description
Topology	Topology name. The topology name for base topology is **base**.
MTID	Topology ID. The value of 0 indicates the base topology.
LsId	Link state ID.
AdvId	ID of the advertising router.
NodeType	Node type: • **Network**—Network node. • **Router**—Router node.
Mask	Network mask. Its value is 0 for a router node.
SPFLinkCnt	Number of SPF links.
Distance	Cost to the root node.
VlinkData	Destination address of virtual link packets.
ParentLinkCnt	Number of parent links.
NodeFlag	Node flag: • **I**—The node is in initialization state. • **A**—The node is on the candidate list. • **S**—The node is on the SPF tree. • **R**—The node is directly connected to the root node. • **D**—The node is to be deleted. • **T**—The node is the tunnel destination. This flag is not supported in the current software version.
NextHop	Next hop.
Interface	Output interface.
BkNextHop	Backup next hop.
LinkId	Link ID.
LinkType	Link type: • **RT2RT**—Router to router. • **NET2RT**—Network to router. • **RT2NET**—Router to network.
LinkCost	Link cost.

Field	Description
NextHopCnt	Number of next hops.
LinkData	Link data.
LinkNewCost	New link cost.
LinkFlag	Link flag: • **I**—The link is in initialization state. • **P**—The peer is the parent node. • **C**—The peer is the child node. • **D**—The link is to be deleted. • **H**—The next hop is changed. • **V**—When the peer node is deleted or added, the peer node is not on the SPF tree or is deleted. • **N**—The link is newly added, and both end nodes are on the SPF tree. • **G**—The link is on the area change list.

display ospf statistics

Use **display ospf statistics** to display OSPF statistics.

Syntax

display ospf [*process-id*] **statistics** [**error** | **packet** [**hello** | *interface-type interface-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays OSPF statistics for all OSPF processes.

error: Displays error statistics. If you do not specify this keyword, the command displays OSPF packet, LSA, and route statistics.

packet: Displays OSPF packet statistics.

hello: Displays statistics of the sent and received hello packets. If you do not specify this keyword, the command displays statistics of all types of sent and received OSPF packets.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify this argument, the command displays statistics for all interfaces.

Examples

Display OSPF statistics.

```
<Sysname> display ospf statistics

          OSPF Process 1 with Router ID 2.2.2.2
                  Statistics
```

```
I/O statistics
 Type                    Input     Output
 Hello                   61        122
 DB Description          2          3
 Link-State Req          1          1
 Link-State Update       3          3
 Link-State Ack          3          2

LSAs originated by this router
 Router  : 4
 Network : 0
 Sum-Net : 0
 Sum-Asbr: 0
 External: 0
 NSSA    : 0
 Opq-Link: 0
 Opq-Area: 0
 Opq-As  : 0

LSAs originated: 4  LSAs received: 7

Routing table:
  Intra area: 2  Inter area: 3  ASE/NSSA: 0
```

Table 34 Command output

Field	Description
I/O statistics	Statistics about input/output packets and LSAs.
Type	OSPF packet type.
Input	Packets received.
Output	Packets sent.
Hello	Hell packet.
DB Description	Database Description packet.
Link-State Req	Link-State Request packet.
Link-State Update	Link-State Update packet.
Link-State Ack	Link-State Acknowledge packet.
LSAs originated by this router	LSAs originated by this router.
Router	Number of Type-1 LSAs originated.
Network	Number of Type-2 LSAs originated.
Sum-Net	Number of Type-3 LSAs originated.
Sum-Asbr	Number of Type-4 LSAs originated.
External	Number of Type-5 LSAs originated.
NSSA	Number of Type-7 LSAs originated.
Opq-Link	Number of Type-9 LSAs originated.

Field	Description
Opq-Area	Number of Type-10 LSAs originated.
Opq-As	Number of Type-11 LSAs originated.
LSA originated	Number of LSAs originated.
LSA received	Number of LSAs received.
Routing table	Routing table information.
Intra area	Number of intra-area routes.
Inter area	Number of inter-area routes.
ASE/NSSA	Number of ASE/NSSA routes.

Display OSPF error statistics.

```
<Sysname> display ospf statistics error

          OSPF Process 1 with Router ID 192.168.1.112
                  OSPF Packet Error Statistics

 0          : Router ID confusion         0          : Bad packet
 0          : Bad version                 0          : Bad checksum
 0          : Bad area ID                 0          : Drop on unnumbered link
 0          : Bad virtual link            0          : Bad authentication type
 0          : Bad authentication key      0          : Packet too small
 0          : Neighbor state low          0          : Transmit error
 0          : Interface down              0          : Unknown neighbor
 0          : HELLO: Netmask mismatch     0          : HELLO: Hello-time mismatch
 0          : HELLO: Dead-time mismatch   0          : HELLO: Ebit option mismatch
 0          : HELLO: Mbit option mismatch 0          : DD: MTU option mismatch
 0          : DD: Unknown LSA type        0          : DD: Ebit option mismatch
 0          : ACK: Bad ack                0          : ACK: Unknown LSA type
 0          : REQ: Empty request          0          : REQ: Bad request
 0          : UPD: LSA checksum bad       0          : UPD: Unknown LSA type
 0          : UPD: Less recent LSA
```

Table 35 Command output

Field	Description
Router ID confusion	Packets with duplicate router ID.
Bad packet	Packets illegal.
Bad version	Packets with wrong version.
Bad checksum	Packets with wrong checksum.
Bad area ID	Packets with invalid area ID.
Drop on unnumbered link	Packets dropped on the unnumbered interface.
Bad virtual link	Packets on wrong virtual links.
Bad authentication type	Packets with invalid authentication type.
Bad authentication key	Packets with invalid authentication key.

Field	Description
Packet too small	Packets too small in length.
Neighbor state low	Packets received in low neighbor state.
Transmit error	Packets with error when being transmitted.
Interface down	Shutdown times of the interface.
Unknown neighbor	Packets received from unknown neighbors.
HELLO: Netmask mismatch	Hello packets with mismatched mask.
HELLO: Hello-time mismatch	Hello packets with mismatched hello timer.
HELLO: Dead-time mismatch	Hello packets with mismatched dead timer.
HELLO: Ebit option mismatch	Hello packets with mismatched E-bit in the option field.
HELLO: Mbit option mismatch	Hello packets with mismatched M-bit in the option field.
DD: MTU option mismatch	DD packets with mismatched MTU.
DD: Unknown LSA type	DD packets with unknown LSA type.
DD: Ebit option mismatch	DD packets with mismatched E-bit in the option field.
ACK: Bad ack	Bad LSAck packets for LSU packets.
ACK: Unknown LSA type	LSAck packets with unknown LSA type.
REQ: Empty request	LSR packets with no request information.
REQ: Bad request	Bad LSR packets.
UPD: LSA checksum bad	LSU packets with wrong LSA checksum.
UPD: Unknown LSA type	LSU packets with unknown LSA type.
UPD: Less recent LSA	LSU packets without the most recent LSA.

Display OSPF packet statistics for all processes and interfaces.

```
<Sysname> display ospf statistics packet

          OSPF Process 100 with Router ID 192.168.1.59
                  Packet Statistics

 Waiting to send packet count: 0
        Hello      DD         LSR        LSU        ACK        Total
 Input : 489        6          2          44         40         581
 Output: 492        8          2          45         40         587

 Area: 0.0.0.1
 Interface: 20.1.1.1 (Vlan-interface100)
        DD         LSR        LSU        ACK        Total
 Input : 0          0          0          0          0
 Output: 0          0          0          0          0

 Interface: 100.1.1.1 (Vlan-interface100)
        DD         LSR        LSU        ACK        Total
 Input : 3          1          22         16         42
```

```
Output: 2          1          19         20         42
```

Table 36 Command output

Field	Description
Waiting to send packet count	Number of packets waiting to be sent.
Total	Total number of packets.
Input	Number of received packets.
Output	Number of sent packets.
Area	Area ID.
Interface	Interface address and interface name.

Display statistics of the sent and received hello packets.

```
<Sysname> display ospf statistics packet hello

        OSPF Process 1 with Router ID 100.1.1.1
                Hello Statistics
 Total sent                            : 4
 Total sent failed                     : 0
 Sent after one and a half intervals   : 0
 Total received                        : 2
 Total received dropped                : 0
 Received after one and a half intervals: 0
```

Table 37 Command output

Field	Description
Total sent	Total number of hello packets sent.
Total sent failed	Total number of hello packets that failed to be sent.
Sent after one and a half intervals	Total number of hello packets sent at intervals greater than 1.5 times the hello interval.
Total received	Total number of hello packets received.
Total received dropped	Total number of received hello packets that were dropped.
Received after one and a half intervals	Total number of hello packets received at intervals greater than 1.5 times the hello interval.

Related commands

`reset ospf statistics`

display ospf troubleshooting

Use **`display ospf troubleshooting`** to display OSPF neighbor relationship troubleshooting information.

NOTE:

This command is supported only in Release 6342 and later.

Syntax

display ospf troubleshooting

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display OSPF neighbor relationship troubleshooting information.

```
<Sysname> display ospf troubleshooting

                OSPF troubleshooting Information
Total count: 3
Time                  Sequence   Description
2019-09-02 19:31:28   101        The state of OSPF 1 peer 1.1.1.1 changed to DOWN because
the interface went down or MTU changed. Please check the interface state and MTU settings
(Interface: Vlan10, neighbor address: 10.1.1.1)
2019-09-02 15:33:28   100       The state of OSPF 1 peer 1.1.1.1 changed to Down because
dead timer expired. Please check the connection to the neighbor (Interface: Vlan10,
neighbor address: 10.1.1.1; ping result: 5 packets in total, 5 packets timed out; CPU usage:
25.37%; memory usage: 36.49%, memory state: normal).
2019-09-02 15:28:00   99        The state of OSPF 1 peer 1.1.1.1 changed to Down because
the BFD session went down. Please check the BFD session information.
```

Table 38 Command output

Field	Description
Total count	Total number of OSPF neighbor relationship troubleshooting entries.
Time	Time when the OSPF neighbor was disconnected. The most recent entry is displayed first.
Sequence	Sequence number of the OSPF neighbor relationship troubleshooting entry.
Description	OSPF neighbor relationship troubleshooting information, including the OSPF process ID, neighbor ID, reason, and recommended action. • The state of OSPF 1 peer 1.1.1.1 changed to DOWN because OSPF interface parameters changed. Please check the interface parameters (Interface: Vlan10, peer address: 10.1.1.1). • The state of OSPF 1 peer 1.1.1.1 changed to DOWN because the OSPF process was reset. • The state of OSPF 1 peer 1.1.1.1 changed to DOWN because the OSPF process was deleted. • The state of OSPF 1 peer 1.1.1.1 changed to DOWN because the OSPF area was deleted. • The state of OSPF 1 peer 1.1.1.1 changed to DOWN because OSPF was disabled (Interface: Vlan10, peer address: 10.1.1.1). • The state of OSPF 1 peer 1.1.1.1 changed to DOWN because OSPF packet receiving and sending are disabled (Interface:

	Vlan10, peer address: 10.1.1.1). • The state of OSPF 1 peer 1.1.1.1 changed to DOWN because the interface address was deleted or OSPF was disabled on interface. Please check the interface settings (Interface: Vlan10, peer address: 10.1.1.1). • The state of OSPF 1 peer 1.1.1.1 changed to DOWN because the interface went down or MTU changed. Please check the interface state and MTU settings (Interface: Vlan10, peer address: 10.1.1.1). • The state of OSPF 1 peer 1.1.1.1 changed to DOWN because the virtual link was deleted or the route it relies on was deleted. Please check the virtual link and the route it relies on (Interface: Vlan10, peer address: 10.1.1.1). • The state of OSPF 1 peer 1.1.1.1 changed to DOWN because the virtual link interface went down or the virtual link settings were deleted. Please check the virtual link and the route it relies on (Interface: Vlan10, peer address: 10.1.1.1). • The state of OSPF 1 peer 1.1.1.1 changed to DOWN because the sham link was deleted or the route it relies on was deleted. Please check the sham link and the route it relies on (Interface: Vlan10, peer address: 10.1.1.1). • The state of OSPF 1 peer 1.1.1.1 changed to DOWN because the dead timer expired. Please check the connection to the peer (Interface: Vlan10, peer address: 10.1.1.1; ping result: 5 packets in total, 5 packets timed out; CPU usage: 25.37%; memory usage: 36.49%, memory state: normal). • The state of OSPF 1 peer 1.1.1.1 changed to DOWN because the dead timer expired. Please check the connection to the peer (Interface: Vlan10, peer address: 10.1.1.1; ping result: ping was not executed because of the disabled MTP; CPU usage: 25.37%; memory usage: 36.49%, memory state: normal). • The state of OSPF 1 peer 1.1.1.1 changed to DOWN because the dead timer expired. Please check the connection to the peer (Interface: Vlan10, peer address: 10.1.1.1; ping result: waitting for the ping to execute; CPU usage: 25.37%; memory usage: 36.49%, memory state: normal). • The state of OSPF 1 peer 1.1.1.1 changed to DOWN because the stub configuration changed in area 0.0.0.1. • The state of OSPF 1 peer 1.1.1.1 changed to DOWN because the NSSA configuration changed in area 0.0.0.1. • The state of OSPF 1 peer 1.1.1.1 changed to DOWN because the Opaque LSA capability configuration changed. • The state of OSPF 1 peer 1.1.1.1 changed to DOWN because the out-of-band resynchronization capability configuration changed. • The state of OSPF 1 peer 1.1.1.1 changed to DOWN because the BFD session went down. Please check the BFD session information. • The state of OSPF 1 peer 1.1.1.1 changed to INIT because a 1-way hello packet was received. Please check the OSPF peer state on the remote end (Interface: Vlan10, peer address: 10.1.1.1). • The state of OSPF 1 peer 1.1.1.1 changed to DOWN because database-filter configuration changed or database-filter ACL configuration changed. Please check the OSPF database-filter and its ACL configuration (Interface: Vlan10, peer address: 10.1.1.1). • The state of OSPF 1 peer 1.1.1.1 changed to EXSTART because a BadLSReq event was triggered upon the request for a nonexistent LSA. Please check the local OSPF LSDB

	and the OSPF request queue on the remote end (Interface: Vlan10, peer address: 10.1.1.1, LSA type: 5, LSID: 91.1.1.0, AdvRouter: 5.5.5.5). • The state of OSPF 1 peer 1.1.1.1 changed to EXSTART because the LSA requested and then learned is the same as that in local. Please check the OSPF request queue and the specified LSA on both ends (Interface: Vlan10, peer address: 10.1.1.1; LSA type: 5, LSID: 91.1.1.0, AdvRouter: 5.5.5.5). • The state of OSPF 1 peer 1.1.1.1 changed to EXSTART because the LSA requested and then learned is older than that in local. Please check the OSPF request queue and the specified LSA on both ends (Interface: Vlan10, peer address: 10.1.1.1; LSA type: 5, LSID: 91.1.1.0, AdvRouter: 5.5.5.5). • The state of OSPF 1 peer 1.1.1.1 changed to EXSTART because a SeqNumberMismatch event was triggered upon the receipt of a non-retransmitted DD packet from the Loading or Full peer during the DD retransmit interval. Please check the OSPF peer state and LSDB on the remote end (Interface: Vlan10, peer address: 10.1.1.1). • The state of OSPF 1 peer 1.1.1.1 changed to EXSTART because a SeqNumberMismatch event was triggered by the change of the OSPF peer's capability to external attribute. Please check the DD packets transmitted on both ends (Interface: Vlan10, peer address: 10.1.1.1). • The state of OSPF 1 peer 1.1.1.1 changed to EXSTART because a SeqNumberMismatch event was triggered by the OSPF peer's multi-topology attribute change. Please check the multi-topology capability configuration on the remote end (Interface: Vlan10, peer address: 10.1.1.1). • The state of OSPF 1 peer 1.1.1.1 changed to EXSTART because a SeqNumberMismatch event was triggered upon the receipt of a retransmitted DD packet from the Loading or Full peer after the DD retransmit interval expired. Please check the OSPF peer state and LSDB on the remote end (Interface: Vlan10, peer address: 10.1.1.1). • The state of OSPF 1 peer 1.1.1.1 changed to EXSTART because a SeqNumberMismatch event was triggered by the change of the OSPF peer's capability to receive AS external LSA. Please check the area configuration (Interface: Vlan10, peer address: 10.1.1.1). • The state of OSPF 1 peer 1.1.1.1 changed to EXSTART because a SeqNumberMismatch event was triggered by the master-slave relationship change. Please check the DD packets transmitted on both ends (Interface: Vlan10, peer address: 10.1.1.1). • The state of OSPF 1 peer 1.1.1.1 changed to EXSTART because a SeqNumberMismatch event was triggered upon the receipt of an unexpected initial DD packet after DD transmission started. Please check the DD packets transmitted on both ends (Interface: Vlan10, peer address: 10.1.1.1). • The state of OSPF 1 peer 1.1.1.1 changed to EXSTART because a SeqNumberMismatch event was triggered upon the receipt of a DD packet with a wrong sequence number from the slave. Please check the DD packets transmitted on both ends (Interface: Vlan10, peer address: 10.1.1.1). • The state of OSPF 1 peer 1.1.1.1 changed to EXSTART because a SeqNumberMismatch event was triggered upon the receipt of a DD packet with a wrong sequence number from the master. Please check the DD packets transmitted on both ends (Interface: Vlan10, peer address: 10.1.1.1). • The state of OSPF 1 peer 1.1.1.1 changed to EXSTART

	because a SeqNumberMismatch event was triggered upon the receipt of a DD packet containing local opaque LSA without enabling the opaque capability. Please check the specified LSA on the remote end and the opaque capability configuration on both ends (Interface: Vlan10, peer address: 10.1.1.1). • The state of OSPF 1 peer 1.1.1.1 changed to EXSTART because a SeqNumberMismatch event was triggered upon the receipt of a DD packet containing area opaque LSA without enabling the opaque capability. Please check the specified LSA on the remote end and the opaque capability configuration on both ends (Interface: Vlan10, peer address: 10.1.1.1). • The state of OSPF 1 peer 1.1.1.1 changed to EXSTART because a SeqNumberMismatch event was triggered upon the receipt of a DD packet containing AS opaque LSA without enabling the opaque capability. Please check the specified LSA on the remote end and the opaque capability configuration on both ends (Interface: Vlan10, peer address: 10.1.1.1). • The state of OSPF 1 peer 1.1.1.1 changed to EXSTART because a SeqNumberMismatch event was triggered upon the receipt of a DD packet containing NSSA external LSA in a non-NSSA area. Please check the specified LSA on the remote end and the area configuration on both ends (Interface: Vlan10, peer address: 10.1.1.1). • The state of OSPF 1 peer 1.1.1.1 changed to EXSTART because a SeqNumberMismatch event was triggered upon the receipt of a DD packet containing invalid LSA. Please check the specified LSA on the remote end (Interface: Vlan10, peer address: 10.1.1.1). • The state of OSPF 1 peer 1.1.1.1 changed to EXSTART because a SeqNumberMismatch event was triggered upon the receipt of a DD packet containing AS external LSA in the stub area or on the virtual link. Please check the specified LSA on the remote end and the area configuration on both ends (Interface: Vlan10, peer address: 10.1.1.1).

Related commands

`reset ospf troubleshooting`

display ospf vlink

Use **`display ospf vlink`** to display OSPF virtual link information.

Syntax

`display ospf` [*`process-id`*] **`vlink`**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

`process-id`: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays the OSPF virtual link information for all OSPF processes.

Examples

Display OSPF virtual link information.

```
<Sysname> display ospf vlink


          OSPF Process 1 with Router ID 3.3.3.3
                  Virtual Links

 Virtual-link Neighbor-ID  -> 2.2.2.2, Neighbor-State: Full
 Interface: 10.1.2.1 (Vlan-interface100)
 Cost: 1562  State: P-2-P  Type: Virtual
 Transit Area: 0.0.0.1
 Timers: Hello 10 , Dead 40 , Retransmit 5 , Transmit Delay 1
 MD5 authentication enabled.
    The last key is 3.
    The rollover is in progress, 2 neighbor(s) left.
```

Table 39 Command output

Field	Description
Virtual-link Neighbor-ID	ID of the neighbor on the virtual link.
Neighbor-State	Neighbor state: Down, Init, 2-Way, ExStart, Exchange, Loading, Full.
Interface	IP address and name of the local interface on the virtual link.
Cost	Interface route cost.
State	Interface state.
Type	Virtual link.
Transit Area	Transit area ID.
Timers	Values of timers (in seconds): **Hello**, **Dead**, and **Retransmit**.
Transmit Delay	LSA transmission delay on the interface, in seconds.
Simple authentication enabled	Simple authentication is enabled.
MD5 authentication enabled	MD5/HMAC-MD5 authentication is enabled.
The last key is *xx*	The most recent MD5 authentication key ID is *xx*.
The rollover is in progress, *xx* neighbor(s) left	Key rollover for MD5/HMAC-MD5 authentication is in progress. The number of neighbors that have not completed rollover is *xx*.

display router id

Use **display router id** to display the global router ID.

Syntax

display router id

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the global router ID.

```
<Sysname> display router id
         Configured router ID is 1.1.1.1
```

dscp

Use **dscp** to set the DSCP value for outgoing OSPF packets.

Use **undo dscp** to restore the default.

Syntax

dscp *dscp-value*

undo dscp

Default

The DSCP value for outgoing OSPF packets is 48.

Views

OSPF view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies the DSCP value in the range of 0 to 63 for outgoing OSPF packets.

Examples

Set the DSCP value for outgoing OSPF packets to 63 in OSPF process 1.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] dscp 63
```

enable link-local-signaling

Use **enable link-local-signaling** to enable the OSPF link-local signaling (LLS) capability.

Use **undo enable link-local-signaling** to disable the OSPF LLS capability.

Syntax

enable link-local-signaling

undo enable link-local-signaling

Default

OSPF link-local signaling capability is disabled.

Views

OSPF view

Predefined user roles

network-admin

Examples

Enable link-local signaling for OSPF process 1.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] enable link-local-signaling
```

enable out-of-band-resynchronization

Use **enable out-of-band-resynchronization** to enable the OSPF out-of-band resynchronization (OOB-Resynch) capability.

Use **undo enable out-of-band-resynchronization** to disable the OSPF out-of-band resynchronization capability.

Syntax

enable out-of-band-resynchronization

undo enable out-of-band-resynchronization

Default

The OSPF out-of-band resynchronization capability is disabled.

Views

OSPF view

Predefined user roles

network-admin

Usage guidelines

Before you configure this command, enable the link-local signaling capability.

Examples

Enable the out-of-band resynchronization capability for OSPF process 1.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] enable link-local-signaling
[Sysname-ospf-1] enable out-of-band-resynchronization
```

Related commands

enable link-local-signaling

event-log

Use **event-log** to set the number of OSPF logs.

Use **undo event-log** to remove the configuration.

Syntax

event-log { **hello** { **received** [**abnormal** | **dropped**] | **sent** [**abnormal** | **failed**] } | **lsa-flush** | **peer** | **spf** } **size** *count*

undo event-log { **hello** { **received** [**abnormal** | **dropped**] | **sent** [**abnormal** | **failed**] } | **lsa-flush** | **peer** | **spf** } **size**

Default

The device can generate a maximum of 100 logs for each type.

Views

OSPF view

Predefined user roles

network-admin

Parameters

hello: Specifies the number of logs for received or sent hello packets.

received: Specifies the number of logs for received hello packets.

sent: Specifies the number of logs for sent hello packets.

abnormal: Specifies the number of logs for abnormal hello packets received or sent at intervals greater than or equal to 1.5 times the hello interval.

dropped: Specifies the number of logs for received hello packets that were dropped.

failed: Specifies the number of logs for hello packets that failed to be sent.

lsa-flush: Specifies the number of LSA aging logs.

peer: Specifies the number of neighbor logs.

spf: Specifies the number of route calculation logs.

size *count*: Specifies the number of OSPF logs, in the range of 0 to 65535.

Examples

Set the number of route calculation logs to 50 in OSPF process 100.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] event-log spf size 50
```

fast-reroute (OSPF view)

Use **fast-reroute** to configure OSPF FRR.

Use **undo fast-reroute** to restore the default.

Syntax

fast-reroute { **lfa** [**abr-only**] | **route-policy** *route-policy-name* }

undo fast-reroute

Default

OSPF FRR is disabled.

Views

OSPF view

Predefined user roles

network-admin

Parameters

lfa: Uses the LFA algorithm to calculate a backup next hop for all routes.

abr-only: Uses the next hop of the route to the ABR as the backup next hop.

route-policy *route-policy-name*: Uses a routing policy to designate a backup next hop. The *route-policy-name* argument is a case-sensitive string of 1 to 63 characters.

Usage guidelines

When both OSPF FRR and PIC are configured, OSPF FRR takes effect.

Do not use the **fast-reroute lfa** command together with the **vlink-peer** command.

Examples

Enable FRR to calculate a backup next hop for all routes by using LFA algorithm in OSPF process 1.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] fast-reroute lfa
```

filter (OSPF area view)

Use **filter** to configure OSPF to filter inbound/outbound Type-3 LSAs on an ABR.

Use **undo filter** to disable Type-3 LSA filtering.

Syntax

filter { *ipv4-acl-number* | **prefix-list** *prefix-list-name* | **route-policy** *route-policy-name* } { **export** | **import** }

undo filter { **export** | **import** }

Default

Type-3 LSAs are not filtered.

Views

OSPF area view

Predefined user roles

network-admin

Parameters

ipv4-acl-number: Specifies an IPv4 ACL by its number in the range of 2000 to 3999 to filter inbound/outbound Type-3 LSAs.

prefix-list-name: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter inbound/outbound Type-3 LSAs.

route-policy-name: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to filter inbound/outbound Type-3 LSAs.

export: Filters Type-3 LSAs advertised to other areas.

import: Filters Type-3 LSAs advertised into the local area.

Usage guidelines

This command applies only to an ABR.

Examples

Use IP prefix list **my-prefix-list** to filter inbound Type-3 LSAs. Use basic ACL 2000 to filter outbound Type-3 LSAs in OSPF Area 1.

```
<Sysname> system-view
```

```
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] filter prefix-list my-prefix-list import
[Sysname-ospf-100-area-0.0.0.1] filter 2000 export
```

filter-policy export (OSPF view)

Use **filter-policy export** to configure OSPF to filter redistributed routes.

Use **undo filter-policy export** to remove the configuration.

Syntax

filter-policy { *ipv4-acl-number* | **prefix-list** *prefix-list-name* } **export** [*protocol* [*process-id*]]

undo filter-policy export [*protocol* [*process-id*]]

Default

OSPF does not filter redistributed routes.

Views

OSPF view

Predefined user roles

network-admin

Parameters

ipv4-acl-number: Specifies an IPv4 ACL by its number in the range of 2000 to 3999 to filter redistributed routes by destination address.

prefix-list-name: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter redistributed routes by destination address.

protocol: Filters routes redistributed from the specified routing protocol. If you do not specify this argument, the command filters all redistributed routes.

process-id: Specifies a process by its ID in the range of 1 to 65535. This argument is available only when the *protocol* argument is **rip** or **ospf**.

Usage guidelines

To use an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL using one of the following methods:

- To deny/permit a route with the specified destination, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* command.
- To deny/permit a route with the specified destination and mask, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* **destination** *dest-addr dest-wildcard* command.

The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the subnet mask of the destination address. For the mask configuration to take effect, specify a contiguous subnet mask.

Examples

Configure OSPF process 100 to filter redistributed routes by using basic ACL 2000.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule deny source 192.168.10.0 0.0.0.255
```

```
[Sysname-acl-ipv4-basic-2000] quit
[Sysname] ospf 100
[Sysname-ospf-100] filter-policy 2000 export
```

Configure advanced ACL 3000 to permit only route 113.0.0.0/16. Configure OSPF process 100 to filter redistributed routes by using advanced ACL 3000.

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule 10 permit ip source 113.0.0.0 0 destination 255.255.0.0
0
[Sysname-acl-ipv4-adv-3000] rule 100 deny ip
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] ospf 100
[Sysname-ospf-100] filter-policy 3000 export
```

Related commands

import-route

filter-policy import (OSPF view)

Use **filter-policy import** to configure OSPF to filter routes calculated using received LSAs.

Use **undo filter-policy import** to restore the default.

Syntax

filter-policy { *ipv4-acl-number* [**gateway** *prefix-list-name*] | **gateway** *prefix-list-name* | **prefix-list** *prefix-list-name* [**gateway** *prefix-list-name*] | **route-policy** *route-policy-name* } **import**

undo filter-policy import

Default

OSPF does not filter routes calculated using received LSAs.

Views

OSPF view

Predefined user roles

network-admin

Parameters

ipv4-acl-number: Specifies an IPv4 ACL by its number in the range of 2000 to 3999 to filter received routes by destination.

gateway *prefix-list-name*: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter received routes by next hop.

prefix-list *prefix-list-name*: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter received routes by destination.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to filter received routes.

Usage guidelines

To use an advanced ACL (with a number from 3000 to 3999) in the command or in the specified routing policy, configure the ACL in one of the following ways:

- To deny/permit a route with the specified destination, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* command.
- To deny/permit a route with the specified destination and mask, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* **destination** *dest-addr dest-wildcard* command.

The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the subnet mask of the destination address. For the mask configuration to take effect, specify a contiguous subnet mask.

Examples

Use basic ACL 2000 to filter received routes.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule deny source 192.168.10.0 0.0.0.255
[Sysname-acl-ipv4-basic-2000] quit
[Sysname] ospf 100
[Sysname-ospf-100] filter-policy 2000 import
```

Configure advanced ACL 3000 to permit only route 113.0.0.0/16. Use ACL 3000 to filter received routes.

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule 10 permit ip source 113.0.0.0 0 destination 255.255.0.0
0
[Sysname-acl-ipv4-adv-3000] rule 100 deny ip
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] ospf 100
[Sysname-ospf-100] filter-policy 3000 import
```

graceful-restart (OSPF view)

Use **graceful-restart** to enable OSPF GR.

Use **undo graceful-restart** to disable OSPF GR.

Syntax

graceful-restart [**ietf** | **nonstandard**] [**global** | **planned-only**] *

undo graceful-restart

Default

OSPF GR is disabled.

Views

OSPF view

Predefined user roles

network-admin

Parameters

ietf: Enables IETF GR.

nonstandard: Enables non-IETF GR.

global: Enables global GR. In global GR mode, a GR process can be completed only when all GR helpers exist. A GR process fails if a GR helper fails (for example, the interface connected to the GR helper goes down). If you do not specify this keyword, the command enables partial GR. In partial GR mode, a GR process can be completed if a GR helper exists.

planned-only: Enables only planned GR. If you do not specify this keyword, the command enables both planned GR and unplanned GR.

Usage guidelines

GR includes planned GR and unplanned GR.

- **Planned GR**—Manually restarts OSPF by using the **reset ospf process** command or performs an active/standby process switchover by using the **placement reoptimize** command. Before OSPF restart or active/standby switchover, the GR restarter sends Grace-LSAs to GR helpers.
- **Unplanned GR**—OSPF restarts or an active/standby switchover occurs because of device failure. Before OSPF restart or active/standby switchover, the GR restarter does not send Grace-LSAs to GR helpers.

Before enabling IETF GR for OSPF, enable Opaque LSA advertisement and reception with the **opaque-capability enable** command.

Before enabling non-IETF GR for OSPF, enable OSPF LLS with the **enable link-local-signaling** command and OOB-Resynch with the **enable out-of-band-resynchronization** command.

If you do not specify the **nonstandard** or **ietf** keyword, this command enables non-IETF GR for OSPF.

OSPF GR and OSPF NSR are mutually exclusive. Do not configure the **graceful-restart** command and the **non-stop-routing** command at the same time.

Examples

Enable IETF GR for OSPF process 1.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] opaque-capability enable
[Sysname-ospf-1] graceful-restart ietf
```

Enable non-IETF GR for OSPF process 1.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] enable link-local-signaling
[Sysname-ospf-1] enable out-of-band-resynchronization
[Sysname-ospf-1] graceful-restart nonstandard
```

Related commands

enable link-local-signaling

enable out-of-band-resynchronization

opaque-capability enable

graceful-restart helper enable

Use **graceful-restart helper enable** to enable OSPF GR helper capability.

Use **undo graceful-restart helper enable** to disable OSPF GR helper capability.

Syntax

graceful-restart helper enable [**planned-only**]

undo graceful-restart helper enable

Default

OSPF GR helper capability is enabled.

Views

OSPF view

Predefined user roles

network-admin

Parameters

planned-only: Enables only planned GR for the GR helper. If you do not specify this keyword, the command enables both planned GR and unplanned GR for the GR helper.

Usage guidelines

The **planned-only** keyword is available only for the IETF GR helper.

Examples

Enable GR helper capability for OSPF process 1.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] graceful-restart helper enable
```

graceful-restart helper strict-lsa-checking

Use **graceful-restart helper strict-lsa-checking** to enable strict LSA checking capability for GR helper.

Use **undo graceful-restart helper strict-lsa-checking** to disable strict LSA checking capability for GR helper.

Syntax

graceful-restart helper strict-lsa-checking

undo graceful-restart helper strict-lsa-checking

Default

Strict LSA checking capability for GR helper is disabled.

Views

OSPF view

Predefined user roles

network-admin

Usage guidelines

When an LSA change on the GR helper is detected, the GR helper device exits the GR helper mode.

Examples

Enable strict LSA checking capability for GR helper in OSPF process 1.

```
<Sysname> system-view
[Sysname] ospf 1
```

```
[Sysname-ospf-1] graceful-restart helper strict-lsa-checking
```

graceful-restart interval (OSPF view)

Use **graceful-restart interval** to set the GR interval.

Use **undo graceful-restart interval** to restore the default.

Syntax

graceful-restart interval *interval*

undo graceful-restart interval

Default

The GR interval is 120 seconds.

Views

OSPF view

Predefined user roles

network-admin

Parameters

interval: Specifies the GR interval in the range of 40 to 1800 seconds.

Usage guidelines

For GR restart to succeed, the value of the GR restart interval cannot be smaller than the maximum OSPF neighbor dead time of all the OSPF interfaces.

Examples

Set the GR interval for OSPF process 1 to 100 seconds.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] graceful-restart interval 100
```

Related commands

ospf timer dead

host-advertise

Use **host-advertise** to advertise a host route.

Use **undo host-advertise** to remove a host route.

Syntax

host-advertise *ip-address cost-value*

undo host-advertise *ip-address*

Default

No host route is advertised.

Views

OSPF area view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address of a host.

cost-value: Specifies a cost for the route, in the range of 1 to 65535.

Examples

Advertise host route 1.1.1.1 with a cost of 100.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 0
[Sysname-ospf-100-area-0.0.0.0] host-advertise 1.1.1.1 100
```

import-route (OSPF view)

Use **import-route** to redistribute AS-external routes from another routing protocol.

Use **undo import-route** to disable route redistribution from another routing protocol.

Syntax

import-route { **direct** | **static** } [**cost** *cost-value*] | **nssa-only** | **route-policy** *route-policy-name* | **tag** *tag* | **type** *type*] *

import-route { **ospf** | **rip** } [*process-id* | **all-processes**] [**allow-direct** | **cost** *cost-value* | **nssa-only** | **route-policy** *route-policy-name* | **tag** *tag* | **type** *type*] *

undo import-route { **direct** | { **ospf** | **rip** } [*process-id* | **all-processes**] | **static** }

Default

OSPF does not redistribute AS-external routes from any other routing protocol.

Views

OSPF view

Predefined user roles

network-admin

Parameters

direct: Redistributes direct routes.

ospf: Redistributes OSPF routes.

rip: Redistributes RIP routes.

static: Redistributes static routes.

process-id: Specifies a process by its ID in the range of 1 to 65535. The default is 1.

all-processes: Redistributes routes from all the processes of the specified routing protocol.

allow-direct: Redistributes the networks of the local interfaces enabled with the specified routing protocol. If you do not specify this keyword, the networks of the local interfaces are not redistributed. If you specify both the **allow-direct** keyword and the **route-policy** *route-policy-name* option, make sure the **if-match** rule defined in the routing policy does not conflict with the **allow-direct** keyword. For example, if you specify the **allow-direct** keyword, do not configure the **if-match route-type** rule for the routing policy. Otherwise, the **allow-direct** keyword does not take effect.

cost *cost-value*: Specifies a route cost in the range of 0 to 16777214. If you do not specify a cost, the cost of a redistributed route is 1.

nssa-only: Limits the route advertisement to the NSSA area by setting the P-bit of Type-7 LSAs to 0. If you do not specify this keyword, the P-bit of Type-7 LSAs is set to 1. If the router acts as both an ASBR and an ABR and **FULL** state neighbors exist in the backbone area, the P-bit is set to 0. This keyword applies to NSSA routers.

route-policy *route-policy-name*: Specifies a routing policy to filter redistributed routes. The *route-policy-name* argument is a case-sensitive string of 1 to 63 characters.

tag *tag*: Specifies a tag for external LSAs, in the range of 0 to 4294967295. The default is 1.

type *type*: Specifies a cost type, 1 or 2. The default is 2.

Usage guidelines

This command redistributes routes destined for other ASs from another protocol. AS external routes include the following types:

- **Type-1 external routes**—Have high credibility. The cost of Type-1 external routes is comparable with the cost of OSPF internal routes. The cost of a Type-1 external route equals the cost from the router to the ASBR plus the cost from the ASBR to the external route's destination.
- **Type-2 external routes**—Have low credibility. OSPF considers the cost from the ASBR to the destination of a Type-2 external route is much bigger than the cost from the ASBR to an OSPF internal router. The cost of a Type-2 external route equals the cost from the ASBR to the Type-2 external route's destination.

The **import-route** command redistributes only active routes. To display information about active routes, use the **display ip routing-table protocol** command. The **import-route** command cannot redistribute default external routes.

The **import-route nssa-only** command redistributes AS-external routes in Type-7 LSAs only into the NSSA area.

The **undo import-route** { **ospf** | **rip** } **all-processes** command removes only the configuration made by the **import-route** { **ospf** | **rip** } **all-processes** command, instead of the configuration made by the **import-route** { **ospf** | **rip** } *process-id* command.

Examples

Redistribute routes from RIP process 40 and specify the type, tag, and cost as 2, 33, and 50 for redistributed routes.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] import-route rip 40 type 2 tag 33 cost 50
```

Related commands

default-route-advertise (OSPF view)

ispf enable (OSPF view)

Use **ispf enable** to enable OSPF incremental SPF (ISPF).

Use **undo ispf enable** to disable OSPF ISPF.

Syntax

ispf enable

undo ispf enable

Default

OSPF ISPF is enabled.

Views

OSPF view

Predefined user roles

network-admin

Usage guidelines

Upon topology changes, ISPF recomputes only the affected part of the SPT, instead of the entire SPT.

Examples

Disable ISPF for OSPF process 100.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] undo ispf enable
```

log-peer-change

Use **log-peer-change** to enable logging for OSPF neighbor state changes.

Use **undo log-peer-change** to disable logging for OSPF neighbor state changes.

Syntax

log-peer-change

undo log-peer-change

Default

Logging for OSPF neighbor state changes is enabled.

Views

OSPF view

Predefined user roles

network-admin

Usage guidelines

This command enables output of OSPF neighbor state changes to the information center. The information center processes the logs according to user-defined output rules (whether and where to output logs). For more information about the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Disable logging for neighbor state changes for OSPF process 100.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] undo log-peer-change
```

lsa-arrival-interval

Use **lsa-arrival-interval** to set the LSA arrival interval.

Use **undo lsa-arrival-interval** to restore the default.

Syntax

lsa-arrival-interval *interval*

undo lsa-arrival-interval

Default

The LSA arrival interval is 1000 milliseconds.

Views

OSPF view

Predefined user roles

network-admin

Parameters

interval: Specifies the LSA arrival interval in the range of 0 to 60000 milliseconds.

Usage guidelines

If an LSA that has the same LSA type, LS ID, and originating router ID as the previous LSA is received within the interval, OSPF discards the LSA. This feature helps avoid overuse of system resources due to frequent network changes.

As a best practice, set the interval with the **lsa-arrival-interval** command to be smaller than or equal to the minimum interval set with the **lsa-generation-interval** command.

Examples

Set the LSA arrival interval to 200 milliseconds.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] lsa-arrival-interval 200
```

Related commands

lsa-generation-interval

lsa-generation-interval

Use **lsa-generation-interval** to set the OSPF LSA generation interval.

Use **undo lsa-generation-interval** to restore the default.

Syntax

lsa-generation-interval *maximum-interval* [*minimum-interval* [*incremental-interval*]]

undo lsa-generation-interval

Default

The maximum interval is 5 seconds, the minimum interval is 50 milliseconds, and the incremental interval is 200 milliseconds.

Views

OSPF view

Predefined user roles

network-admin

Parameters

maximum-interval: Specifies the maximum LSA generation interval in the range of 1 to 60 seconds.

minimum-interval: Specifies the minimum LSA generation interval in the range of 10 to 60000 milliseconds.

incremental-interval: Specifies the LSA generation incremental interval in the range of 10 to 60000 milliseconds.

Usage guidelines

When network changes are infrequent, LSAs are generated at the minimum interval. If network changes become frequent, the LSA generation interval is incremented by the incremental interval × 2^{n-2} for each generation until the maximum interval is reached. The value *n* is the number of generation times.

The minimum interval and the incremental interval cannot be greater than the maximum interval.

Examples

Set the maximum LSA generation interval to 2 seconds, minimum interval to 100 milliseconds, and incremental interval to 100 milliseconds.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] lsa-generation-interval 2 100 100
```

Related commands

lsa-arrival-interval

lsdb-overflow-interval

Use **lsdb-overflow-interval** to set the interval that OSPF exits overflow state.

Use **undo lsdb-overflow-interval** to restore the default.

Syntax

lsdb-overflow-interval *interval*

undo lsdb-overflow-interval

Default

The OSPF exit overflow interval is 300 seconds.

Views

OSPF view

Predefined user roles

network-admin

Parameters

interval: Specifies the interval that OSPF exits overflow state, in the range of 0 to 2147483647 seconds.

Usage guidelines

When the number of LSAs in the LSDB exceeds the upper limit, the LSDB is in an overflow state. In this state, OSPF does not receive any external LSAs and deletes the external LSAs generated by itself to save system resources.

You can configure the interval that OSPF exits overflow state. An interval of 0 indicates that the timer is not started and OSPF does not exit overflow state.

Examples

Set the OSPF exit overflow interval to 10 seconds.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] lsdb-overflow-interval 10
```

lsdb-overflow-limit

Use **lsdb-overflow-limit** to set the upper limit of external LSAs in the LSDB.

Use **undo lsdb-overflow-limit** to restore the default.

Syntax

lsdb-overflow-limit *number*

undo lsdb-overflow-limit

Default

The number of external LSAs is not limited.

Views

OSPF view

Predefined user roles

network-admin

Parameters

number: Specifies the upper limit of external LSAs in the LSDB, in the range of 1 to 1000000.

Examples

Set the upper limit of external LSAs to 400000.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] lsdb-overflow-limit 400000
```

network (OSPF area view)

Use **network** to enable OSPF on the interface attached to the specified network in the area.

Use **undo network** to disable OSPF for the interface attached to the specified network in the area.

Syntax

network *ip-address wildcard-mask*

undo network *ip-address wildcard-mask*

Default

OSPF is not enabled for any interface.

Views

OSPF area view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address of a network.

wildcard-mask: Specifies the wildcard mask of the IP address. For example, the wildcard mask of mask 255.0.0.0 is 0.255.255.255.

Usage guidelines

This command enables OSPF on the interface attached to the specified network. The interface's primary IP address must be in the specified network. If only the interface's secondary IP address is in the network, the interface cannot run OSPF.

Examples

Specify the interface whose primary IP address is on network 131.108.20.0/24 to run OSPF in Area 2.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 2
[Sysname-ospf-100-area-0.0.0.2] network 131.108.20.0 0.0.0.255
```

Related commands

ospf

non-stop-routing

Use **non-stop-routing** to enable OSPF NSR.

Use **undo non-stop-routing** to disable OSPF NSR.

Syntax

non-stop-routing

undo non-stop-routing

Default

OSPF NSR is disabled.

Views

OSPF view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only for the current process. As a best practice, enable OSPF NSR for each process if multiple OSPF processes exist.

OSPF NSR and OSPF GR are mutually exclusive. Do not configure the **non-stop-routing** command and the **graceful-restart** command at the same time.

Examples

Enable NSR for OSPF process 100.

```
<Sysname> system-view
[Sysname] ospf 100
```

```
[Sysname-ospf-100] non-stop-routing
```

nssa (OSPF area view)

Use **nssa** to configure an area as an NSSA area.

Use **undo nssa** to restore the default.

Syntax

nssa [**default-route-advertise** [**cost** *cost-value* | **nssa-only** | **route-policy** *route-policy-name* | **type** *type*] * | **no-import-route** | **no-summary** | **suppress-fa** | [[[**translate-always**] [**translate-ignore-checking-backbone**]] | **translate-never**] | **translator-stability-interval** *value*] *

undo nssa [**default-route-advertise** [**cost** | **nssa-only** | **route-policy** | **type**] * | **no-import-route** | **no-summary** | **suppress-fa** | [**translate-always** | **translate-never**] | **translator-stability-interval**] *

Default

No area is configured as an NSSA area.

Views

OSPF area view

Predefined user roles

network-admin

Parameters

default-route-advertise: Used on an NSSA ABR or an ASBR only. With this keyword, an NSSA ABR redistributes a default route in a Type-7 LSA into the NSSA area. The ABR redistributes a default route regardless of whether a default route exists in the routing table. With this keyword, an ASBR redistributes a default route in a Type-7 LSA only when the default route exists in the routing table.

cost *cost-value*: Specifies a cost for the default route, in the range of 0 to 16777214. If you do not specify this option, the default cost specified by the **default-cost** command applies.

nssa-only: Limits the default route advertisement to the NSSA area by setting the P-bit of Type-7 LSAs to 0. By default, the P-bit of Type-7 LSAs is set to 1. If the router acts as both an ASBR and an ABR and **FULL** state neighbors exist in the backbone area, the P-bit is set to 0.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters. When a default route exists in the routing table and the routing policy is matched, the command redistributes a default route in a Type-7 LSA into the OSPF routing domain. The routing policy modifies values in the Type-7 LSA.

type *type*: Specifies a type for the Type-7 LSA, 1 or 2. If you do not specify this option, the default type specified by the **default type** command applies.

no-import-route: Used on an NSSA ABR to control the **import-route** command to not redistribute routes into the NSSA area.

no-summary: Used only on an ABR to advertise a default route in a Type-3 summary LSA into the NSSA area and to not advertise other summary LSAs into the area. The area is a totally NSSA area.

suppress-fa: Suppresses the forwarding address in the Type-7 LSAs from being placed in the Type-5 LSAs.

translate-always: Always translates Type-7 LSAs to Type-5 LSAs. This keyword takes effect only on an NSSA ABR.

translate-ignore-checking-backbone: Ignores checking for FULL state neighbors in the backbone area during the translator election in the NSSA area.

translate-never: Never translates Type-7 LSAs to Type-5 LSAs. This keyword takes effect only on an NSSA ABR.

translator-stability-interval *value*: Specifies the stability interval of the translator. During the interval, the translator can maintain its translating capability after another device becomes the new translator. The *value* argument is the stability interval in the range of 0 to 900 seconds and defaults to 0. A value of 0 means the translator does not maintain its translating capability when a new translator arises.

Usage guidelines

All routers attached to an NSSA area must be configured with the **nssa** command in area view.

If you specify the **translate-ignore-checking-backbone** keyword for an ABR, you must also specify the keyword for other ABRs in the NSSA area. This ensures that a translator can be elected among the ABRs.

Examples

Configure Area 1 as an NSSA area.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] nssa
```

Related commands

default-cost (OSPF area view)

opaque-capability enable

Use **opaque-capability enable** to enable opaque LSA advertisement and reception.

Use **undo opaque-capability** to disable opaque LSA advertisement and reception.

Syntax

opaque-capability enable

undo opaque-capability

Default

The feature is enabled.

Views

OSPF view

Predefined user roles

network-admin

Usage guidelines

After the opaque LSA advertisement and reception capability is enabled, OSPF can receive and advertise Type-9, Type-10, and Type-11 opaque LSAs.

Examples

Disable opaque LSA advertisement and reception.

```
<Sysname> system-view
[Sysname] ospf 100
```

```
[Sysname-ospf-100] undo opaque-capability
```

ospf

Use **ospf** to enable OSPF and enter OSPF view.

Use **undo ospf** to disable OSPF.

Syntax

ospf [*process-id* | **router-id** *router-id*] *

undo ospf [*process-id*]

Default

OSPF is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535.

router-id *router-id*: Specifies an OSPF router ID in dotted decimal notation.

Usage guidelines

You can enable multiple OSPF processes on a router and specify different router IDs for them.

Enable an OSPF process before performing other tasks.

Examples

Enable OSPF process 100 and specify router ID 10.10.10.1.

```
<Sysname> system-view
[Sysname] ospf 100 router-id 10.10.10.1
[Sysname-ospf-100]
```

ospf area

Use **ospf area** to enable OSPF on an interface.

Use **undo ospf area** to disable OSPF on an interface.

Syntax

ospf *process-id* **area** *area-id* [**exclude-subip**]

undo ospf *process-id* **area** [**exclude-subip**]

Default

OSPF is not enabled on an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535.

area-id: Specifies an area by its ID, an IP address or a decimal integer in the range of 0 to 4294967295 that is translated into the IP address format.

exclude-subip: Excludes secondary IP addresses. If you do not specify this keyword, the command enables OSPF also on secondary IP addresses.

Usage guidelines

The **ospf area** command has a higher priority than the **network** command.

If the specified process and area do not exist, the command creates the process and area. Disabling an OSPF process on an interface does not delete the OSPF process or the area.

Examples

Enable OSPF process 1 on VLAN-interface 10 that is in Area 2 and exclude secondary IP addresses.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf 1 area 2 exclude-subip
```

Related commands

network

ospf authentication-mode

Use **ospf authentication-mode** to set the authentication mode and key on an interface.

Use **undo ospf authentication-mode** to remove specified configuration.

Syntax

For MD5/HMAC-MD5 authentication:

ospf authentication-mode { **hmac-md5** | **md5** } *key-id* { **cipher** | **plain** } *string*

undo ospf authentication-mode { **hmac-md5** | **md5** } *key-id*

For simple authentication:

ospf authentication-mode simple { **cipher** | **plain** } *string*

undo ospf authentication-mode simple

Default

No authentication is performed for an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

hmac-md5: Specifies HMAC-MD5 authentication.

md5: Specifies MD5 authentication.

simple: Specifies simple authentication.

key-id: Specifies a key by its ID in the range of 1 to 255.

cipher: Specifies a key in encrypted form.

plain: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive.

- In simple authentication mode, the plaintext form of the key is a string of 1 to 8 characters. The encrypted form of the key is a string of 33 to 41 characters.
- In MD5/HMAC-MD5 authentication mode, the plaintext form of the key is a string of 1 to 16 characters. The encrypted form of the key is a string of 33 to 53 characters.

Usage guidelines

To establish or maintain adjacencies, interfaces attached to the same network segment must have the same authentication mode and key.

If MD5 or HMAC-MD5 authentication is configured, you can configure multiple keys, each having a unique key ID and key string. To minimize the risk of key compromise, use only one key for an interface and delete the old key after key replacement.

To replace the key used for MD5 or HMAC-MD5 authentication on an interface, you must configure the new key before removing the old key from each router. OSPF uses the key rollover mechanism to ensure that the routers can pass authentication before the replacement is complete on the interface. After you configure a new key on a router, the router sends copies of the same packet, each authenticated by a different key, including the new key and the keys in use. This practice continues until the router detects that all its neighbors have the new key.

Examples

On VLAN-interface 10, enable MD5 authentication, and set the interface key ID to 15 and the key to **123456** in plaintext form.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf authentication-mode md5 15 plain 123456
```

On VLAN-interface 10, enable simple authentication, and set the key to **123456** in plaintext form.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf authentication-mode simple plain 123456
```

Related commands

authentication-mode

ospf bfd enable

Use **ospf bfd enable** to enable BFD on an OSPF interface.

Use **undo ospf bfd enable** to disable BFD on an OSPF interface.

Syntax

ospf bfd enable [**echo**]

undo ospf bfd enable

Default

BFD for OSPF is disabled.

Views

Interface view

Predefined user roles

network-admin

Parameters

echo: Enables BFD single-hop echo detection. If you do not specify this keyword, the command enables BFD bidirectional control detection.

Examples

Enable BFD for OSPF on VLAN-interface 11.

```
<Sysname> system-view
[Sysname] ospf
[Sysname-ospf-1] area 0
[Sysname-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.255.255
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] ospf bfd enable
```

ospf cost (interface view)

Use **ospf cost** to set an OSPF cost for an interface.

Use **undo ospf cost** to restore the default.

Syntax

ospf cost *cost-value*

undo ospf cost

Default

An interface computes its OSPF cost according to the interface bandwidth. For a loopback interface, the cost is 0.

Views

Interface view

Predefined user roles

network-admin

Parameters

cost-value: Specifies an OSPF cost in the range of 0 to 65535 for a loopback interface, and in the range of 1 to 65535 for other interfaces.

Usage guidelines

If you do not execute this command, the interface automatically computes its OSPF cost.

Examples

Set the OSPF cost on VLAN-interface 10 to 65.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf cost 65
```

Related commands

bandwidth-reference

ospf database-filter

Use **ospf database-filter** to filter outbound LSAs on an interface.

Use **undo ospf database-filter** to restore the default.

Syntax

ospf database-filter { **all** | { **ase** [**acl** *ipv4-acl-number*] | **nssa** [**acl** *ipv4-acl-number*] | **summary** [**acl** *ipv4-acl-number*] } * }

undo ospf database-filter

Default

The outbound LSAs are not filtered on the interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

all: Filters all outbound LSAs except the Grace LSAs.

ase: Filters outbound Type-5 LSAs.

nssa: Filters outbound Type-7 LSAs.

summary: Filters outbound Type-3 LSAs.

acl *ipv4-acl-number*: Specifies an IPv4 ACL by its number in the range of 2000 to 3999.

Usage guidelines

To use an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL using one of the following methods:

- To deny/permit LSAs with the specified link state ID, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* command.
- To deny/permit LSAs with the specified link state ID and mask, use the **rule** [*rule-id*] { **deny** | **permit** } **ip source** *sour-addr sour-wildcard* **destination** *dest-addr dest-wildcard* command.

The **source** keyword specifies the link state ID of an LSA and the **destination** keyword specifies the subnet mask of the LSA. For the mask configuration to take effect, specify a contiguous subnet mask.

If the neighbor has already received an LSA to be filtered, the LSA still exists in the LSDB of the neighbor after you execute the command.

Examples

Filter all outbound LSAs (except the Grace LSAs) on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf database-filter all
```

On VLAN-interface 20, configure ACL 2000, 2100, and 2200 to filter outbound Type-5, Type-7, and Type-3 LSAs, respectively.

```
<Sysname> system-view
[Sysname] interface vlan-interface 20
```

```
[Sysname- Vlan-interface20] ospf database-filter ase acl 2000 nssa acl 2100 summary acl
2200
```

Related commands

`database-filter peer` (OSPF view)

ospf dr-priority

Use **`ospf dr-priority`** to set the router priority for DR/BDR election on an interface.

Use **`undo ospf dr-priority`** to restore the default value.

Syntax

`ospf dr-priority` *`priority`*

`undo ospf dr-priority`

Default

The router priority is 1.

Views

Interface view

Predefined user roles

network-admin

Parameters

`priority`: Specifies the router priority for the interface, in the range of 0 to 255.

Usage guidelines

The greater the value, the higher the priority for DR/BDR election. If a device has a priority of 0, it will not be elected as a DR or BDR.

Examples

Set the router priority on VLAN-interface 10 to 8.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf dr-priority 8
```

ospf fast-reroute lfa-backup

Use **`ospf fast-reroute lfa-backup`** to enable LFA on an interface.

Use **`undo ospf fast-reroute lfa-backup`** to disable LFA on an interface.

Syntax

`ospf fast-reroute lfa-backup`

`undo ospf fast-reroute lfa-backup`

Default

LFA is enabled on an interface.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

An interface enabled with LFA can be selected as a backup interface. After you disable LFA on the interface, it cannot be selected as a backup interface.

Examples

Disable VLAN-interface 11 from calculating a backup next hop by using the LFA algorithm.

```
<Sysname> system-view
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] undo ospf fast-reroute lfa-backup
```

ospf lsu-flood-control

Use **ospf lsu-flood-control** to enable OSPF to limit the LSU transmit rate.

Use **undo ospf lsu-flood-control** to disable OSPF to limit LSU transmit rate.

Syntax

ospf lsu-flood-control [*interval count*]

undo ospf lsu-flood-control

Default

OSPF does not limit the LSU transmit rate.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the LSU transmit interval in the range of 10 to 1000 milliseconds. The default value is 30.

count: Specifies the maximum number of LSUs that can be sent at each interval, in the range of 1 to 1000. The default value is 50.

Usage guidelines

During LSDB synchronization, if the local router has multiple neighbors, it must send many LSUs to each neighbor. When a neighbor receives excessive LSUs within a short time period, the following events might occur:

- The performance of the neighbor is degraded because too many system resources are occupied for LSU packet processing.
- The neighbor drops hello packets used for maintaining the neighbor relationship because it is busy dealing with the LSUs. As a result, the neighbor relationship is torn down. To reestablish a relationship to the neighbor, the local router must send more LSUs to the neighbor. This exacerbates the performance degradation.

To prevent this problem, execute this command to limit the global LSU transmit rate.

Inappropriate use of this command might cause abnormal routing. As a best practice, execute this command with the default values.

Examples

Enable OSPF to limit the LSU transmit rate, and configure all OSPF interfaces to send 60 LSUs every 40 milliseconds.

```
<Sysname> system-view
[Sysname] ospf lsu-flood-control 40 60
```

ospf mib-binding

Use **ospf mib-binding** to bind an OSPF process to the public MIB.

Use **undo ospf mib-binding** to restore the default.

Syntax

ospf mib-binding *process-id*

undo ospf mib-binding

Default

The public MIB is bound to the OSPF process with the smallest process ID.

Views

System view

Predefined user roles

network-admin

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535.

Usage guidelines

To access information or data about an OSPF process in **RFC4750-OSPF.MIB**, use this command. To access information or data about an OSPF process in a private MIB for the device, you do not need to use this command. You can access information or data about all OSPF processes in the private MIBs.

If the specified process ID does not exist, a notification is displayed to report that the MIB binding configuration has failed.

Deleting an OSPF process that has been bound to the public MIB unbinds the OSPF process from the MIB, and re-binds the MIB to the OSPF process with the smallest process ID.

Examples

Bind OSPF process 100 to the public MIB.

```
<Sysname> system-view
[Sysname] ospf mib-binding 100
```

ospf mtu-enable

Use **ospf mtu-enable** to enable an interface to add the interface MTU into DD packets.

Use **undo ospf mtu-enable** to restore the default.

Syntax

ospf mtu-enable

undo ospf mtu-enable

Default

The MTU in DD packets is 0.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

After you configure this command, the interface checks whether the MTU in a received DD packet is greater than its own MTU. If yes, the interface discards the packet.

Examples

Enable VLAN-interface 10 to add the interface MTU value into DD packets.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf mtu-enable
```

ospf network-type

Use **ospf network-type** to specify the network type for an interface.

Use **undo ospf network-type** to restore the default.

Syntax

ospf network-type { **broadcast** | **nbma** | **p2mp** [**unicast**] | **p2p** [**peer-address-check**] }

undo ospf network-type

Default

The network type of an interface is broadcast.

Views

Interface view

Predefined user roles

network-admin

Parameters

broadcast: Specifies the network type as broadcast.

nbma: Specifies the network type as NBMA.

p2mp: Specifies the network type as P2MP.

unicast: Specifies the P2MP interface to unicast OSPF packets. By default, a P2MP interface multicasts OSPF packets.

p2p: Specifies the network type as P2P.

peer-address-check: Checks whether the peer interface and the local interface are on the same network segment. Two P2P interfaces can establish a neighbor relationship only when they are on the same network segment.

Usage guidelines

If a router on a broadcast network does not support multicast, configure the network type for the connected interfaces as NBMA.

When the network type of an interface is NBMA or P2MP unicast, you must use the **peer** command to specify the neighbor.

If only two routers run OSPF on a network, you can configure the network type for the connected interfaces as P2P.

When the network type of an interface is P2MP unicast, all OSPF packets are unicast by the interface.

Examples

Specify the OSPF network type for VLAN-interface 10 as NBMA.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf network-type nbma
```

Related commands

ospf dr-priority

ospf packet-size

Use **ospf packet-size** to set the maximum length of OSPF packets that can be sent by an interface.

Use **undo ospf packet-size** to restore the default.

Syntax

ospf packet-size *value*

undo ospf packet-size

Default

The maximum length of OSPF packets that an interface can send equals the interface's MTU.

Views

Interface view

Predefined user roles

network-admin

Parameters

value: Specifies the maximum length of OSPF packets that can be sent by an interface, in the range of 500 to 10000 bytes.

Usage guidelines

The interface chooses the smaller one between the value set in this command and the interface MTU, and uses it as the maximum length of OSPF packets that can be sent.

Examples

Set the maximum length of OSPF packets that can be sent by VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan 10
[Sysname-Vlan-interface10] ospf packet-size 1000
```

ospf prefix-suppression

Use **ospf prefix-suppression** to disable an OSPF interface from advertising all its IP prefixes, except for the prefixes of secondary IP addresses.

Use **undo ospf prefix-suppression** to restore the default.

Syntax

ospf prefix-suppression [**disable**]

undo ospf prefix-suppression

Default

Prefix suppression is disabled.

Views

Interface view

Predefined user roles

network-admin

Parameters

disable: Disables prefix suppression for an interface.

Usage guidelines

To disable prefix suppression for an interface associated with an OSPF process that has been enabled with prefix suppression, use the **ospf prefix-suppression disable** command on that interface.

Examples

Enable prefix suppression for VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf prefix-suppression
```

Related commands

prefix-suppression

ospf primary-path-detect bfd

Use **ospf primary-path-detect bfd** to enable BFD for primary link failure detection for OSPF.

Use **undo ospf primary-path-detect bfd** to disable BFD for primary link failure detection for OSPF.

Syntax

ospf primary-path-detect bfd { **ctrl** | **echo** }

undo ospf primary-path-detect bfd

Default

BFD is disabled for primary link failure detection for OSPF.

Views

Interface view

Predefined user roles

network-admin

Parameters

ctrl: Enables BFD control packet mode.

echo: Enables BFD echo packet mode.

Usage guidelines

This command enables OSPF PIC or OSPF FRR to use BFD to detect primary link failures.

Examples

On VLAN-interface 10, enable BFD control packet mode for OSPF FRR.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] fast-reroute lfa
[Sysname-ospf-1] quit
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf primary-path-detect bfd ctrl
```

On VLAN-interface 11, enable BFD echo packet mode for OSPF PIC.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] pic additional-path-always
[Sysname-ospf-1] quit
[Sysname] bfd echo-source-ip 1.1.1.1
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] ospf primary-path-detect bfd echo
```

ospf timer dead

Use **ospf timer dead** to set the neighbor dead interval.

Use **undo ospf timer dead** to restore the default.

Syntax

ospf timer dead *seconds*

undo ospf timer dead

Default

The dead interval is 40 seconds for broadcast and P2P interfaces. The dead interval is 120 seconds for P2MP and NBMA interfaces.

Views

Interface view

Predefined user roles

network-admin

Parameters

seconds: Specifies the dead interval in the range of 1 to 2147483647 seconds.

Usage guidelines

If an interface receives no hello packet from a neighbor within the dead interval, the interface considers the neighbor down.

The dead interval on an interface is a minimum of four times the hello interval. Routers attached to the same segment must have the same dead interval.

Examples

Set the dead interval for VLAN-interface 10 to 60 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf timer dead 60
```

Related commands

ospf timer hello

ospf timer hello

Use **ospf timer hello** to set the hello interval on an interface.

Use **undo ospf timer hello** to restore the default.

Syntax

ospf timer hello *seconds*

undo ospf timer hello

Default

The hello interval is 10 seconds for P2P and broadcast interfaces, and is 30 seconds for P2MP and NBMA interfaces.

Views

Interface view

Predefined user roles

network-admin

Parameters

seconds: Specifies the hello interval in the range of 1 to 65535 seconds.

Usage guidelines

The shorter the hello interval, the faster the topology converges, and the more resources are consumed. Make sure the hello interval on two neighboring interfaces is the same.

Examples

Set the hello interval on VLAN-interface to 20 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf timer hello 20
```

Related commands

ospf timer dead

ospf timer poll

Use **ospf timer poll** to set the poll interval on an NBMA interface.

Use **undo ospf timer poll** to restore the default.

Syntax

ospf timer poll *seconds*

undo ospf timer poll

Default

The poll interval is 120 seconds on an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

seconds: Specifies the poll interval in the range of 1 to 2147483647 seconds.

Usage guidelines

When an NBMA interface finds its neighbor is down, it sends hello packets at the poll interval.

The poll interval must be a minimum of four times the hello interval.

Examples

Set the poll timer interval on VLAN-interface 10 to 130 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf timer poll 130
```

Related commands

ospf timer hello

ospf timer retransmit

Use **ospf timer retransmit** to set the LSA retransmission interval on an interface.

Use **undo ospf timer retransmit** to restore the default.

Syntax

ospf timer retransmit *seconds*

undo ospf timer retransmit

Default

The LSA retransmission interval is 5 seconds on an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

seconds: Specifies the LSA retransmission interval in the range of 1 to 3600 seconds.

Usage guidelines

After sending an LSA, an interface waits for an acknowledgment packet. If the interface receives no acknowledgment within the retransmission interval, it retransmits the LSA.

To avoid unnecessary retransmissions, set an appropriate retransmission interval. For example, you can set a large retransmission interval value on a low-speed link.

Examples

Set the LSA retransmission interval to 8 seconds on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf timer retransmit 8
```

ospf trans-delay

Use **ospf trans-delay** to set the LSA transmission delay on an interface.

Use **undo ospf trans-delay** to restore the default.

Syntax

ospf trans-delay *seconds*

undo ospf trans-delay

Default

The LSA transmission delay is 1 second.

Views

Interface view

Predefined user roles

network-admin

Parameters

seconds: Specifies the LSA transmission delay in the range of 1 to 3600 seconds.

Usage guidelines

Each LSA in the LSDB has an age that is incremented by 1 every second, but the age does not change during transmission. Adding a transmission delay into the age time is important in low speed networks.

Examples

Set the LSA transmission delay to 3 seconds on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf trans-delay 3
```

ospf troubleshooting max-number

Use **ospf troubleshooting max-number** to set the maximum number of OSPF neighbor relationship troubleshooting entries.

Use **undo ospf troubleshooting max-number** to restore the default.

NOTE:

This command is supported only in Release 6342 and later.

Syntax

ospf troubleshooting max-number *number*

undo ospf troubleshooting max-number

Default

The maximum number of OSPF neighbor relationship troubleshooting entries is 100.

Views

System view

Predefined user roles

network-admin

Parameters

number: Specifies the maximum number of OSPF neighbor relationship troubleshooting entries, in the range of 0 to 65535. The value 0 means OSPF does not record neighbor relationship troubleshooting entries.

Examples

Set the maximum number of OSPF neighbor relationship troubleshooting entries to 50.

```
<Sysname> system-view
[Sysname] ospf troubleshooting max-number 50
```

ospf ttl-security

Use **ospf ttl-security** to enable OSPF GTSM for an interface.

Use **undo ospf ttl-security** to disable OSPF GTSM for an interface.

Syntax

ospf ttl-security [**hops** *hop-count* | **disable**]

undo ospf ttl-security

Default

OSPF GTSM is disabled for an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

hops *hop-count*: Specifies the hop limit for checking OSPF packets, in the range of 1 to 254. The default hop limit is 1 for packets from common neighbors, and is 255 for packets from virtual link neighbors.

disable: Disables OSPF GTSM for the interface.

Usage guidelines

GTSM protects the device by comparing the TTL value in the IP header of incoming OSPF packets against a valid TTL range. If the TTL value is within the valid TTL range, the packet is accepted. If not, the packet is discarded.

The valid TTL range is from 255 – the configured hop count + 1 to 255.

When GTSM is configured, the OSPF packets sent by the device have a TTL of 255. To use GTSM, you must configure GTSM on both the local and peer devices. You can specify different *hop-count* values for them.

The **hops** keyword configured in interface view takes precedence over the **hops** keyword configured in OSPF area view.

If the **ttl-security** command is not configured, the **undo ospf ttl-security** command disables GTSM for an interface.

If the **ttl-security** command is configured, the **undo ospf ttl-security** command removes the GTSM configuration for an interface. At the same time, the GTSM configuration for the area applies to the interface. The **ospf ttl-security disable** command disables GTSM for an interface.

If a virtual link exists in an area, you can enable GTSM for the interfaces on the virtual link. If you do not know the interfaces on the virtual link, enable GTSM in area view to prevent packet loss.

Examples

Enable OSPF GTSM for VLAN-interface 10 and set the hop limit to 254.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf ttl-security hops 254
```

Enable GTSM in OSPF area view and disable OSPF GTSM for VLAN-interface 10.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] ttl-security
[Sysname-ospf-100-area-0.0.0.1] quit
[Sysname-ospf-100] quit
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf ttl-security disable
```

Related commands

ttl-security (OSPF area view)

peer (OSPF view)

Use **peer** to specify a neighbor in an NBMA or P2MP network.

Use **undo peer** to remove a neighbor in an NBMA or P2MP network.

Syntax

peer *ip-address* [**cost** *cost-value* | **dr-priority** *priority*]

undo peer *ip-address*

Default

No neighbor is specified.

Views

OSPF view

Predefined user roles

network-admin

Parameters

ip-address: Specifies a neighbor by its IP address.

cost *cost-value*: Specifies the cost to reach the neighbor, in the range of 1 to 65535.

dr-priority *priority*: Specifies the DR priority for the neighbor, in the range of 0 to 255. The default neighbor DR priority is 1.

Usage guidelines

In an NBMA or P2MP network, OSPF packets are sent in unicast, so you must use this command to specify neighbors.

The cost set with the **peer** command applies only to P2MP neighbors. If no cost is specified, the cost to the neighbor equals the local interface's cost.

A router uses the priority set with the **peer** command to determine whether to send a hello packet to the neighbor rather than for DR election. The DR priority set with the **ospf dr-priority** command is used for DR election.

Examples

Specify the neighbor 1.1.1.1.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] peer 1.1.1.1
```

Related commands

ospf dr-priority

pic (OSPF view)

Use **pic** to enable OSPF PIC.

Use **undo pic** to disable OSPF PIC.

Syntax

pic [**additional-path-always**]

undo pic

Default

OSPF PIC is enabled.

Views

OSPF view

Predefined user roles

network-admin

Parameters

additional-path-always: Allows the indirect suboptimal route as the backup route.

Usage guidelines

Prefix Independent Convergence (PIC) enables the device to speed up network convergence by ignoring the number of prefixes. PIC applies only to inter-area routes and external routes.

When both OSPF PIC and OSPF FRR are configured, OSPF FRR takes effect.

Examples

Configure OSPF PIC to support the suboptimal route as the backup route.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] pic additional-path-always
```

preference (OSPF view)

Use **preference** to set a preference for OSPF.

Use **undo preference** to remove the configuration.

Syntax

preference [**ase**] { *preference* | **route-policy** *route-policy-name* } *

undo preference [**ase**]

Default

The preference is 10 for OSPF internal routes and 150 for OSPF external routes (ASE routes).

Views

OSPF view

Predefined user roles

network-admin

Parameters

ase: Specifies a preference for OSPF external routes. If you do not specify this keyword, the command sets a preference for OSPF internal routes.

preference: Specifies the preference value in the range of 1 to 255. A smaller value represents a higher preference.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to set a preference for the specified routes.

Usage guidelines

If multiple routing protocols find routes to the same destination, the router uses the route found by the protocol with the highest preference.

When the **route-policy** *route-policy-name* option is specified, the following preferences take effect:

- For routes matching the routing policy, the preference set in the routing policy takes effect.
- For other routes, the preference set with the **preference** command takes effect.

Examples

Set a preference of 200 for OSPF external routes.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] preference ase 200
```

Set a preference of 100 for OSPF internal routes matching the specified routing policy, and set a preference of 150 for other routes.

```
<Sysname> system-view
[Sysname] ip prefix-list test index 10 permit 100.1.1.0 24
[Sysname] route-policy pre permit node 10
[Sysname-route-policy-pre-10] if-match ip address prefix-list test
[Sysname-route-policy-pre-10] apply preference 100
[Sysname-route-policy-pre-10] quit
[Sysname] ospf 100
[Sysname-ospf-100] preference route-policy pre 150
```

prefix-priority (OSPF view)

Use **prefix-priority** to enable prefix prioritization.

Use **undo prefix-priority** to disable prefix prioritization.

Syntax

prefix-priority route-policy *route-policy-name*

undo prefix-priority

Default

Prefix prioritization is disabled.

Views

OSPF view

Predefined user roles

network-admin

Parameters

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to set a priority for the specified route prefixes.

Usage guidelines

Prefix prioritization enables the device to install prefixes in descending priority order: critical, high, medium, and low. The prefix priorities are assigned through routing policies. When a route is assigned multiple prefix priorities, it uses the highest priority.

By default, the 32-bit OSPF host routes have a medium priority and other routes have a low priority.

Examples

Use a routing policy to assign the medium priority to the specified route prefixes.

```
<Sysname> system-view
[Sysname] ip prefix-list test index 10 permit 100.1.1.0 24
[Sysname] route-policy pre permit node 10
[Sysname-route-policy-pre-10] if-match ip address prefix-list test
[Sysname-route-policy-pre-10] apply prefix-priority medium
[Sysname-route-policy-pre-10] quit
[Sysname] ospf 100
[Sysname-ospf-100] prefix-priority route-policy pre
```

prefix-suppression

Use **prefix-suppression** to disable an OSPF process from advertising all IP prefixes except for the prefixes of loopback interfaces, secondary IP addresses, and passive interfaces.

Use **undo prefix-suppression** to restore the default.

Syntax

prefix-suppression

undo prefix-suppression

Default

An OSPF process advertises all prefixes.

Views

OSPF view

Predefined user roles

network-admin

Usage guidelines

By default, an OSPF interface advertises all of its prefixes in LSAs. To speed up OSPF convergence, you can suppress interfaces from advertising all their prefixes. This feature helps improve network security by preventing IP routing to the suppressed networks.

As a best practice, configure prefix suppression on all OSPF routers if you want to use prefix suppression.

To disable an OSPF process from advertising the prefixes of loopback and passive interfaces, configure prefix suppression on the interfaces by using the **ospf prefix-suppression** command.

When prefix suppression is enabled:

- On P2P and P2MP networks, OSPF does not advertise Type-3 links in Type-1 LSAs. Other routing information can still be advertised to ensure traffic forwarding.
- On broadcast and NBMA networks, the DR generates Type-2 LSAs with a mask length of 32 to suppress network routes. Other routing information can still be advertised to ensure traffic forwarding. If no neighbors exist, the DR also does not advertise the primary IP addresses of interfaces in Type-1 LSAs.

Examples

Enable prefix suppression for OSPF process 1.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] prefix-suppression
```

Related commands

ospf prefix-suppression

reset ospf event-log

Use **reset ospf event-log** to clear OSPF log information.

Syntax

reset ospf [*process-id*] **event-log** [**lsa-flush** | **peer** | **spf**]

Views

User view

Predefined user roles

network-admin

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command clears OSPF log information for all OSPF processes.

lsa-flush: Clears LSA aging log information.

peer: Clears neighbor log information.

spf: Clears route calculation log information.

Usage guidelines

If you do not specify a log type, this command clears all log information.

Examples

Clear OSPF route calculation log information for all OSPF processes.

```
<Sysname> reset ospf event-log spf
```

Related commands

display ospf event-log

reset ospf event-log hello

Use **reset ospf event-log hello** to clear OSPF log information about received or sent hello packets.

NOTE:

This command is supported only in Release 6342 and later.

Syntax

reset ospf [*process-id*] **event-log hello** { **received** [**abnormal** | **dropped**] | **sent** [**abnormal** | **failed**] }

Views

User view

Predefined user roles

network-admin

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify this argument, the command clears OSPF log information for all processes.

received: Specifies log information for received hello packets.

sent: Specifies log information for sent hello packets.

abnormal: Specifies log information for abnormal hello packets received or sent at intervals greater than or equal to 1.5 times the hello interval.

dropped: Specifies log information for received hello packets that were dropped.

failed: Specifies log information for hello packets that failed to be sent.

Examples

Clear sent hello packet log information for all OSPF processes.

```
<Sysname> reset ospf event-log hello sent
```

Related commands

display ospf event-log hello

reset ospf process

Use **reset ospf process** to restart all OSPF processes or a specified process.

Syntax

reset ospf [*process-id*] **process** [**graceful-restart**]

Views

User view

Predefined user roles

network-admin

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify a process, this command restarts all OSPF processes.

graceful-restart: Resets the OSPF process by using GR.

Usage guidelines

The **reset ospf process** command performs the following actions:

- Clears all invalid LSAs without waiting for their timeouts.
- Makes a newly configured router ID take effect.
- Starts a new DR/BDR election.
- Keeps previous OSPF configurations.

The system prompts you to select whether to restart OSPF process upon execution of this command.

Examples

Restart all OSPF processes.

```
<Sysname> reset ospf process
Reset OSPF process? [Y/N]:y
```

reset ospf redistribution

Use **reset ospf redistribution** to restart route redistribution.

Syntax

reset ospf [*process-id*] **redistribution**

Views

User view

Predefined user roles

network-admin

Parameters

process-id: Specifies an OSPF process by its ID in the range of 1 to 65535. If you do not specify a process, this command restarts route redistribution for all OSPF processes.

Examples

Restart route redistribution.

```
<Sysname> reset ospf redistribution
```

reset ospf statistics

Use **reset ospf statistics** to clear OSPF statistics.

Syntax

reset ospf [*process-id*] **statistics**

Views

User view

Predefined user roles

network-admin

Parameters

process-id: Clears the statistics for an OSPF process specified by its ID in the range of 1 to 65535.

Examples

Clear OSPF statistics for all processes.

```
<Sysname> reset ospf statistics
```

Related commands

display ospf statistics

reset ospf troubleshooting

Use **reset ospf troubleshooting** to clear OSPF neighbor relationship troubleshooting information.

NOTE:

This command is supported only in Release 6342 and later.

Syntax

reset ospf troubleshooting

Views

User view

Predefined user roles

network-admin

Examples

Clear OSPF neighbor relationship troubleshooting information.

```
<Sysname> reset ospf troubleshooting
```

Related commands

display ospf troubleshooting

rfc1583 compatible

Use **rfc1583 compatible** to enable compatibility with RFC 1583.

Use **undo rfc1583 compatible** to disable compatibility with RFC 1583.

Syntax

rfc1583 compatible

undo rfc1583 compatible

Default

Compatibility with RFC 1583 is enabled.

Views

OSPF view

Predefined user roles

network-admin

Usage guidelines

RFC 1583 specifies a different method than RFC 2328 for selecting the optimal route to a destination in another AS. When multiple routes are available to the ASBR, OSPF selects the optimal route by using the following procedure:

1. Selects the route with the highest preference.
   - If RFC 2328 is compatible with RFC 1583, all these routes have equal preference.
   - If RFC 2328 is not compatible with RFC 1583, the intra-area route in a non-backbone area is preferred to reduce the burden of the backbone area. The inter-area route and intra-area route in the backbone area have equal preference.
2. Selects the route with lower cost if two routes have equal preference.
3. Selects the route with larger originating area ID if two routes have equal cost.

To avoid routing loops, set identical RFC 1583-compatibility on all routers in a routing domain.

Examples

Disable compatibility with RFC 1583.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] undo rfc1583 compatible
```

router id

Use **router id** to configure a global router ID.

Use **undo router id** to restore the default.

Syntax

router id *router-id*

undo router id

Default

No global router ID is configured.

Views

System view

Predefined user roles

network-admin

Parameters

router-id: Specifies the router ID, in the format of an IPv4 address.

Usage guidelines

OSPF uses a router ID to identify a device. If no router ID is specified, the global router ID is used.

If no global router ID is configured, the highest loopback interface IP address is used as the router ID. If no loopback interface IP address is available, the highest physical interface IP address is used, regardless of the interface status (up or down).

During an active/standby process switchover, the new active process checks whether the previously backed up router ID is valid. If not, the process selects a new router ID.

A new router ID is selected only when the interface IP address used as the router ID is removed or changed. Other events will not trigger a router ID re-selection. For example, router ID re-selection is not triggered in the following situations:

- The interface goes down.
- You change the router ID to the address of a loopback interface after a physical interface address is selected as the router ID.
- A higher interface IP address is configured as the router ID.

After a router ID is changed, you must use the **reset** command to enable it.

Examples

Configure a global router ID as 1.1.1.1.

```
<Sysname> system-view
[Sysname] router id 1.1.1.1
```

silent-interface (OSPF view)

Use **silent-interface** to disable an interface or all interfaces from receiving and sending OSPF packets.

Use **undo silent-interface** to remove the configuration.

Syntax

silent-interface { *interface-type interface-number* | **all** }

undo silent-interface { *interface-type interface-number* | **all** }

Default

An interface can receive and send OSPF packets.

Views

OSPF view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

all: Specifies all interfaces.

Usage guidelines

To disable a network from receiving and sending OSPF routes, use the command on the interface connected to the network.

Examples

Disable VLAN-interface 10 from receiving and sending OSPF packets.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] silent-interface vlan-interface 10
```

snmp trap rate-limit

Use **snmp trap rate-limit** to set the SNMP notification output interval and the maximum number of SNMP notifications that can be output at each interval.

Use **undo snmp trap rate-limit** to restore the default.

Syntax

snmp trap rate-limit interval *trap-interval* **count** *trap-number*

undo snmp trap rate-limit

Default

OSPF outputs a maximum of seven SNMP notifications within 10 seconds.

Views

OSPF view

Predefined user roles

network-admin

Parameters

interval *trap-interval*: Specifies the SNMP notification output interval in the range of 2 to 60 seconds.

count *trap-number*: Specifies the number of SNMP notifications output by OSPF at each interval, in the range of 0 to 300. The value of 0 indicates that OSPF does not output SNMP notifications.

Examples

Configure OSPF to output a maximum of 10 SNMP notifications within 5 seconds.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] snmp trap rate-limit interval 5 count 10
```

snmp-agent trap enable ospf

Use **snmp-agent trap enable ospf** to enable SNMP notifications for OSPF.

Use **undo snmp-agent trap enable ospf** to disable SNMP notifications for OSPF.

Syntax

snmp-agent trap enable ospf [**authentication-failure** | **bad-packet** | **config-error** | **grhelper-status-change** | **grrestarter-status-change** | **if-state-change** | **lsa-maxage** | **lsa-originate** | **lsdb-approaching-overflow** | **lsdb-overflow** | **neighbor-state-change** | **nssatranslator-status-change** | **retransmit** | **virt-authentication-failure** | **virt-bad-packet** | **virt-config-error** | **virt-retransmit** | **virtgrhelper-status-change** | **virtif-state-change** | **virtneighbor-state-change**] *

undo snmp-agent trap enable ospf [**authentication-failure** | **bad-packet** | **config-error** | **grhelper-status-change** | **grrestarter-status-change** | **if-state-change** | **lsa-maxage** | **lsa-originate** | **lsdb-approaching-overflow** | **lsdb-overflow** | **neighbor-state-change** | **nssatranslator-status-change** | **retransmit** | **virt-authentication-failure** | **virt-bad-packet** | **virt-config-error** | **virt-retransmit** | **virtgrhelper-status-change** | **virtif-state-change** | **virtneighbor-state-change**] *

Default

SNMP notifications for OSPF are enabled.

Views

System view

Predefined user roles

network-admin

Parameters

authentication-failure: Specifies notifications about authentication failures on an interface.

bad-packet: Specifies notifications about error messages received on an interface.

config-error: Specifies notifications about error configuration of an interface.

grhelper-status-change: Specifies notifications about GR helper state change.

grrestarter-status-change: Specifies notifications about GR restarter state change.

if-state-change: Specifies notifications about interface state change.

lsa-maxage: Specifies LSA max age notifications.

lsa-originate: Specifies notifications about locally generated LSAs.

lsdb-approaching-overflow: Specifies notifications about approaching LSDB overflows.

lsdb-overflow: Specifies LSDB overflow notifications.

neighbor-state-change: Specifies notifications about neighbor state change.

nssatranslator-status-change: Specifies notifications about NSSA translator state change.

retransmit: Specifies notifications about packets that are received and forwarded on an interface.

virt-authentication-failure: Specifies notifications about authentication failures on a virtual interface.

virt-bad-packet: Specifies notifications about error messages received on a virtual interface.

virt-config-error: Specifies notifications about error configuration of a virtual interface.

virt-retransmit: Specifies notifications about packets that are received and forwarded on a virtual interface.

virtgrhelper-status-change: Specifies notifications about neighbor GR helper state changes of a virtual interface.

virtif-state-change: Specifies notifications about virtual interface state change.

virtneighbor-state-change: Specifies notifications about the neighbor state change of a virtual interface.

Examples

Disable SNMP notifications for OSPF.

```
<Sysname> system-view
[Sysname] undo snmp-agent trap enable ospf
```

spf-schedule-interval (OSPF view)

Use **spf-schedule-interval** to set the OSPF SPF calculation interval.

Use **undo spf-schedule-interval** to restore the default.

Syntax

spf-schedule-interval *maximum-interval* [*minimum-interval* [*incremental-interval*]]

undo spf-schedule-interval

Default

The maximum calculation interval is 5 seconds, the minimum interval is 50 milliseconds, and the incremental interval is 200 milliseconds.

Views

OSPF view

Predefined user roles

network-admin

Parameters

maximum-interval: Specifies the maximum OSPF SPF calculation interval in the range of 1 to 60 seconds.

minimum-interval: Specifies the minimum OSPF SPF calculation interval in the range of 10 to 60000 milliseconds.

incremental-interval: Specifies the incremental OSPF SPF calculation interval in the range of 10 to 60000 milliseconds.

Usage guidelines

Based on the LSDB, an OSPF router uses SPF to calculate a shortest path tree with itself as the root. OSPF uses the shortest path tree to determine the next hop to a destination. By adjusting the SPF calculation interval, you can prevent overconsumption of bandwidth and router resources due to frequent topology changes.

For a stable network, the minimum interval is used. If network changes become frequent, the SPF calculation interval is incremented by the incremental interval × 2^{n-2} for each calculation until the maximum interval is reached. The value *n* is the number of calculation times.

The minimum interval and the incremental interval cannot be greater than the maximum interval.

Examples

Set the maximum SPF calculation interval to 10 seconds, minimum interval to 500 milliseconds, and incremental interval to 300 milliseconds.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] spf-schedule-interval 10 500 300
```

stub (OSPF area view)

Use **stub** to configure an area as a stub area.

Use **undo stub** to restore the default.

Syntax

stub [**default-route-advertise-always** | **no-summary**] *

undo stub

Default

No area is a stub area.

Views

OSPF area view

Predefined user roles

network-admin

Parameters

default-route-advertise-always: Enables the ABR to advertise a default route in a Type-3 LSA into the stub area regardless of whether **FULL**-state neighbors exist in the backbone area. If you do not specify this keyword, the ABR advertises a default route in a Type-3 LSA into the stub area only when a minimum of one **FULL**-state neighbor exists in the backbone area.

no-summary: Enables the ABR to advertise only a default route in a Type-3 LSA into the stub area without advertising any other Type-3 LSAs. The area is a totally stub area.

Usage guidelines

To configure an area as a stub area, use the **stub** command on all routers attached to the area.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure Area 1 as a stub area.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] stub
```

Related commands

default-cost (OSPF area view)

stub-router (OSPF view)

Use **stub-router** to configure a router as a stub router.

Use **undo stub-router** to restore the default.

Syntax

stub-router [**external-lsa** [*max-metric-value*] | **include-stub** | **on-startup** *seconds* | **summary-lsa** [*max-metric-value*]] *

undo stub-router

Default

The router is not configured as a stub router.

Views

OSPF view

Predefined user roles

network-admin

Parameters

external-lsa *max-metric-value*: Specifies a cost for the external LSAs, in the range of 1 to 16777215. The default is 16711680.

include-stub: Specifies the cost of the stub links (link type 3) in Router LSAs to the maximum value 65535.

on-startup *seconds*: Specifies the router as a stub router during reboot, and specifies the timeout time in the range of 5 to 86400 seconds.

summary-lsa *max-metric-value*: Specifies a cost for the Type-3 LSAs, in the range of 1 to 16777215. The default cost value is 16711680.

Usage guidelines

The router LSAs sent by the stub router over different links contain different link type values. A value of 3 represents a link to a stub network, and the cost of the link is not changed. A value of 1, 2, or 4 represents a point-to-point link, a link to a transit network, or a virtual link. The cost of these links is set to 65535. Neighbors on such links will not send packets to the stub router as long as they have a route with a smaller cost.

Examples

Configure a stub router.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] stub-router
```

transmit-pacing

Use **transmit-pacing** to set the LSU transmission interval and the maximum number of LSU packets that can be sent at each interval.

Use **undo transmit-pacing** to restore the default.

Syntax

transmit-pacing interval *interval* **count** *count*

undo transmit-pacing

Default

An OSPF interface sends a maximum of three LSU packets every 20 milliseconds.

Views

OSPF view

Predefined user roles

network-admin

Parameters

interval *interval*: Specifies an interval at which an interface sends LSU packets, in the range of 10 to 1000 milliseconds. If the router has multiple OSPF interfaces, increase this interval to reduce the total number of LSU packets sent by the router every second.

count *count*: Specifies the maximum number of LSU packets sent by an interface at each interval, in the range of 1 to 200. If the router has multiple OSPF interfaces, decrease the maximum number to reduce the total number of LSU packets sent by the router every second.

Examples

Configure all the interfaces running OSPF process 1 to send a maximum of 10 LSU packets every 30 milliseconds.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] transmit-pacing interval 30 count 10
```

ttl-security

Use **ttl-security** to enable OSPF GTSM for an area.

Use **undo ttl-security** to disable OSPF GTSM for an area.

Syntax

ttl-security [**hops** *hop-count*]

undo ttl-security

Default

OSPF GTSM is disabled for an OSPF area.

Views

OSPF area view

Predefined user roles

network-admin

Parameters

hops *hop-count*: Specifies the hop limit for checking OSPF packets, in the range of 1 to 254. The default hop limit is 1 for packets from common neighbors, and is 255 for packets from virtual link neighbors.

Usage guidelines

The GTSM configuration in OSPF area view applies to all OSPF interfaces in the area. GTSM checks OSPF packets from common neighbors and virtual link neighbors. It does not check OSPF packets from sham link neighbors.

GTSM protects the device by comparing the TTL value in the IP header of incoming OSPF packets against a valid TTL range. If the TTL value is within the valid TTL range, the packet is accepted. If not, the packet is discarded.

The valid TTL range is from 255 – the configured hop count + 1 to 255.

When GTSM is configured, the OSPF packets sent by the device have a TTL of 255. To use GTSM, you must configure GTSM on both the local and peer devices. You can specify different *hop-count* values for them.

The **hops** keyword configured in interface view takes precedence over the **hops** keyword configured in OSPF area view.

As a best practice, set the hop limit if a virtual link exists in an area. You can enable GTSM for the interfaces on the virtual link. If you do not know the interfaces on the virtual link, enable GTSM in area view to prevent packet loss.

Examples

Enable OSPF GTSM for OSPF area 1.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] ttl-security
```

Related commands

ospf ttl-security

vlink-peer (OSPF area view)

Use **vlink-peer** to configure a virtual link.

Use **undo vlink-peer** to remove a virtual link.

Syntax

vlink-peer *router-id* [**dead** *seconds* | **hello** *seconds* | { { **hmac-md5** | **md5** } *key-id* { **cipher** | **plain** } *string* | **simple** { **cipher** | **plain** } *string* } | **retransmit** *seconds* | **trans-delay** *seconds*] *

undo vlink-peer *router-id* [**dead** | **hello** | { **hmac-md5** | **md5** } *key-id* | **retransmit** | **simple** | **trans-delay**] *

Default

No virtual links exist.

Views

OSPF area view

Predefined user roles

network-admin

Parameters

router-id: Specifies the router ID of the neighbor on the virtual link.

dead *seconds*: Specifies the dead interval in the range of 1 to 32768 seconds. The default is 40. The dead interval must be identical with that on the virtual link neighbor, and a minimum of four times the hello interval.

hello *seconds*: Specifies the hello interval in the range of 1 to 8192 seconds. The default is 10. It must be identical with the hello interval on the virtual link neighbor.

hmac-md5: Specifies the HMAC-MD5 authentication mode.

md5: Specifies the MD5 authentication mode.

simple: Specifies the simple authentication mode.

key-id: Specifies the key ID for MD5 or HMAC-MD5 authentication, in the range of 1 to 255.

cipher: Specifies a key in encrypted form.

plain: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive.

- In simple authentication mode, the plaintext form of the key is a string of 1 to 8 characters. The encrypted form of the key is a string of 33 to 41 characters.
- In MD5/HMAC-MD5 authentication mode, the plaintext form of the key is a string of 1 to 16 characters. The encrypted form of the key is a string of 33 to 53 characters.

retransmit *seconds*: Specifies the retransmission interval in the range of 1 to 3600 seconds. The default is 5.

trans-delay *seconds*: Specifies the transmission delay interval in the range of 1 to 3600 seconds. The default is 1.

Usage guidelines

As defined in RFC 2328, all non-backbone areas must maintain connectivity to the backbone. You can use the **vlink-peer** command to configure a virtual link to connect an area to the backbone.

When you configure this command, follow these guidelines:

- The smaller the hello interval is, the faster the network converges, and the more network resources are consumed.
- A retransmission interval that is too small can cause unnecessary retransmissions. A large value is appropriate for a low speed link.
- Specify an appropriate transmission delay with the **trans-delay** keyword.

You can specify either MD5/HMAC-MD5 authentication or simple authentication for a virtual link. For MD5/HMAC-MD5 authentication, you can configure multiple keys by executing this command multiple times, and each command must have a unique key ID and key string.

To modify the key of a virtual link, perform the following key rollover configurations:

1. Configure a new MD5/HMAC-MD5 authentication key for the virtual link on the local device. If the new key is not configured on the neighbor device, MD5/HMAC-MD5 authentication key rollover is triggered. During key rollover, OSPF sends multiple packets that contain both the new and old MD5/HMAC-MD5 authentication keys to ensure that the neighbor device can pass the authentication.
2. Configure the new MD5/HMAC-MD5 authentication key on the neighbor device. When the local device receives packets with the new key from the neighbor device, it exits MD5 key rollover.
3. Delete the old MD5/HMAC-MD5 authentication key from the local device and the neighbor. This step helps prevent attacks from devices that use the old key for communication and reduces system resources and bandwidth consumption caused by key rollover.

Examples

Configure a virtual link to the neighbor with router ID 1.1.1.1.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 2
[Sysname-ospf-100-area-0.0.0.2] vlink-peer 1.1.1.1
```

Related commands

authentication-mode

display ospf vlink

Contents

Policy-based routing commands

apply next-hop

Use **apply next-hop** to set next hops.

Use **undo apply next-hop** to remove next hops.

Syntax

apply next-hop { *ip-address* [**direct**] [**track** *track-entry-number*] }&<1-2>

undo apply next-hop [*ip-address*&<1-2>]

Default

No next hops are set.

Views

Policy node view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address of the next hop.

direct: Specifies that the next hop must be directly connected to take effect.

track *track-entry-number*: Specifies a track entry by its number in the range of 1 to 1024.

&<1-2>: Indicates that the argument before it can be entered up to two times.

Usage guidelines

You can specify multiple next hops for backup in one command line or by executing this command multiple times.

With a next hop specified, the **undo apply next-hop** command removes the next hop.

Without any next hop specified, the **undo apply next-hop** command removes all next hops.

Examples

Set a directly-connected next hop of 1.1.1.1.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] apply next-hop 1.1.1.1 direct
```

description

Use **description** to configure a description for a policy node.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

No description is configured for a policy node.

Views

Policy node view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 127 characters.

Examples

Configure the description as **Officeuse** for policy node 1.

```
<Sysname> system-view
[Sysname] policy-based-route 1 permit node 1
[Sysname-pbr-1-1] description Officeuse
```

display ip policy-based-route

Use **display ip policy-based-route** to display PBR policy information.

Syntax

display ip policy-based-route [**policy** *policy-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

policy *policy-name*: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters. If you do not specify a policy, this command displays information for all PBR policies.

Examples

Display all policy information.

```
<Sysname> display ip policy-based-route
Policy name: aaa
  node 1 permit:
    if-match acl 2000
    apply next-hop 1.1.1.1
```

Table 1 Command output

Field	Description
node 1 permit	The match mode of Node 1 is **permit**.
if-match acl	Compares packets with the ACL.
apply next-hop	Specifies a next hop for permitted packets.

Related commands

policy-based-route

display ip policy-based-route interface

Use **display ip policy-based-route interface** to display interface PBR configuration and statistics.

Syntax

display ip policy-based-route interface *interface-type interface-number* [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information on the master device.

Examples

Display PBR configuration and statistics on VLAN-interface 2.

```
<Sysname> display ip policy-based-route interface vlan-interface 2
Policy based routing information for interface Vlan-interface2:
Policy name: aaa
  node 0 deny:
  Matched: 0
  node 1 permit:
    if-match acl 3999
  Matched: 0
  node 2 permit:
    if-match acl 2000
    apply next-hop 2.2.2.2
  Matched: 0
  node 5 permit:
    if-match acl 3101
    apply next-hop 1.1.1.1
  Matched: 0
Total matched: 0
<Sysname> display ip policy-based-route interface vlan-interface 2
Policy based routing information for interface Vlan-interface2:
Policy name: aaa
  node 0 deny:
  Matched: 0
  node 1 permit:
    if-match acl 3999
```

```
  Matched: 0
  node 2 permit:
    if-match acl 2000
    apply next-hop 2.2.2.2
  Matched: 0
  node 5 permit:
    if-match acl 3101
    apply next-hop 1.1.1.1
  Matched: 0
Total matched: 0
```

Table 2 Command output

Field	Description
Policy based routing information for interface *XXXX*(failed)	PBR configuration and statistics on the interface. This field displays **failed** in brackets if none of the nodes in the policy has been successfully issued to the driver. The **failed** status will persist even after the policy is successfully issued. To clear the **failed** status, you must remove the policy from the interface and then apply it on the interface again. **NOTE:** The **failed** status is available on a per-slot basis. To obtain this information, you must specify a slot number when you execute the command. • For a global interface (for example, a VLAN interface), which might have member physical interfaces on multiple slots, specify a slot that contains its member interfaces. • For a physical interface, specify its slot number.
node 0 deny(not support) node 2 permit(no resource)	Match mode of the node, **permit** or **deny**. If a node fails to be issued to the driver, the command displays the cause in brackets, which include: • **not support**—The device does not support the match criteria configured on the node. • **no resource**—No sufficient resources (for example, ACLs) are available for the node. **NOTE:** The cause is available only on a per-slot basis. To obtain this information, you must specify a slot number when you execute the command. • For a global interface (for example, a VLAN interface), which might have member physical interfaces on multiple slots, specify a slot that contains its member interfaces. • For a physical interface, specify its slot number.
if-match acl	Compares packets with the ACL.
apply next-hop	Specifies a next hop for permitted packets.
Matched: 0 (no statistics resource)	Number of successful matches on the node. If the device does not have sufficient resources to count matches, this field displays **no statistics resource** in brackets. **NOTE:** The statistics collection failure cause is available only on a per-slot basis. To obtain this information, you must specify a slot number when you execute the command. • For a global interface (for example, a VLAN interface), which

Field	Description
	might have member physical interfaces on multiple slots, specify a slot that contains its member interfaces. • For a physical interface, specify its slot number.
Total matched	Total number of successful matches on all nodes.

Related commands

reset ip policy-based-route statistics

display ip policy-based-route local

Use **display ip policy-based-route local** to display local PBR configuration and statistics.

Syntax

display ip policy-based-route local [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays local PBR configuration and statistics for the master device.

Examples

Display local PBR configuration and statistics.

```
<Sysname> display ip policy-based-route local
Policy based routing information for local:
Policy name: aaa
  node 0 deny:
  Matched: 0
  node 1 permit:
    if-match acl 3999
  Matched: 0
  node 2 permit:
    if-match acl 2000
    apply next-hop 2.2.2.2
  Matched: 0
  node 5 permit:
    if-match acl 3101
    apply next-hop 1.1.1.1
  Matched: 0
Total matched: 0
```

Table 3 Command output

Field	Description
Policy based routing information for local	Local PBR configuration and statistics.
node 0 deny/node 2 permit	Match mode of the node: permit or deny.
if-match acl	Compares packets with the ACL.
apply next-hop	Specifies a next hop for permitted packets.
Matched: 0	Number of successful matches on the node.
Total matched	Total number of successful matches on all nodes.

Related commands

`reset ip policy-based-route statistics`

display ip policy-based-route setup

Use **`display ip policy-based-route setup`** to display PBR configuration.

Syntax

`display ip policy-based-route setup`

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display PBR configuration.

```
<Sysname> display ip policy-based-route setup
Policy name             Type     Interface
pr01                    Forward  Vlan-interface2
aaa                     Local    N/A
aaa                     Global   N/A
```

Table 4 Command output

Field	Description
Type	Type of the PBR: • **Forward**—Interface PBR. • **Local**—Local PBR. • **Global**—Global PBR.
Interface	Interface where the policy is applied. This field displays **N/A** for local PBR and global PBR.

Related commands

`ip policy-based-route`

if-match acl

Use **if-match acl** to set an ACL match criterion.

Use **undo if-match acl** to restore the default.

Syntax

if-match acl { *acl-number* | **name** *acl-name* }

undo if-match acl

Default

No ACL match criterion is set.

Views

Policy node view

Predefined user roles

network-admin

Parameters

acl-number: Specifies an ACL by its number in the range of 2000 to 2999 for a basic ACL, and in the range of 3000 to 3999 for an advanced ACL.

name *acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters starting with letter *a* to *z* or *A* to *Z*. The ACL name cannot be **all**. For the command to take effect, make sure the specified ACL is a basic or advanced ACL.

Examples

Configure Node 11 of policy **aa** to permit the packets matching ACL 2011.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] if-match acl 2011
```

Configure Node 11 of policy **aa** to permit the packets matching ACL **aaa**.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] if-match acl name aaa
```

ip local policy-based-route

Use **ip local policy-based-route** to specify a policy for local PBR.

Use **undo ip local policy-based-route** to restore the default.

Syntax

ip local policy-based-route *policy-name*

undo ip local policy-based-route

Default

No policy is specified for local PBR.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters. The specified policy must already exist.

Usage guidelines

Local PBR guides the forwarding of locally generated packets, such as ICMP packets generated by using the **ping** command.

Local PBR might affect local services, such as ping and Telnet. When you use local PBR, make sure you fully understand its impact on local services of the device.

You can specify only one policy for local PBR and must make sure the specified policy already exists.

Before you apply a new policy, you must first remove the current policy.

Examples

Configure local PBR based on policy **aaa**.

```
<Sysname> system-view
[Sysname] ip local policy-based-route aaa
```

Related commands

display ip policy-based-route setup

policy-based-route

ip policy-based-route

Use **ip policy-based-route** to specify a policy for interface PBR on an interface.

Use **undo ip policy-based-route** to restore the default.

Syntax

ip policy-based-route *policy-name*

undo ip policy-based-route

Default

No policy is applied to an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters. The specified policy must already exist.

Examples

Apply policy **aaa** to VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ip policy-based-route aaa
```

Related commands

display ip policy-based-route setup

policy-based-route

policy-based-route

Use **policy-based-route** to create a policy node and enter its view, or enter the view of an existing policy node.

Use **undo policy-based-route** to delete a policy or policy node.

Syntax

policy-based-route *policy-name* [**deny** | **permit**] **node** *node-number*

undo policy-based-route *policy-name* [**deny** | **node** *node-number* | **permit**]

Default

No policy nodes exist.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters.

deny: Specifies the match mode for the policy node as **deny**.

permit: Specifies the match mode for the policy node as **permit** (default mode).

node *node-number*: Specifies a policy node by its number. A smaller number has a higher priority. The value range for the *node-number* argument is 0 to 255.

Usage guidelines

A policy that has been applied to an interface or locally cannot be deleted. To delete it, you must first cancel the application.

- If a policy node is specified, the **undo policy-based-route** command deletes the specified policy node.
- If a match mode is specified, the command deletes all nodes configured with the match mode.
- If no policy node or match mode is specified, the command deletes the whole policy.

Examples

Create permit-mode of Node 10 for policy **policy1** and enter its view.

```
<Sysname> system-view
[Sysname] policy-based-route policy1 permit node 10
[Sysname-pbr-policy1-10]
```

Related commands

display ip policy-based-route

ip global policy-based-route

ip local policy-based-route

ip policy-based-route apply

reset ip policy-based-route statistics

Use **reset ip policy-based-route statistics** to clear PBR statistics.

Syntax

reset ip policy-based-route statistics [**policy** *policy-name*]

Views

User view

Predefined user roles

network-admin

Parameters

policy *policy-name*: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters. If you do not specify a policy, this command clears PBR statistics for all policies.

Examples

Clear all PBR statistics.

```
<Sysname> reset ip policy-based-route statistics
```

Related commands

display ip policy-based-route interface

display ip policy-based-route local

Contents

IPv6 static routing commands

delete ipv6 static-routes all

Use **delete ipv6 static-routes all** to delete all IPv6 static routes.

Syntax

delete ipv6 static-routes all

Views

System view

Predefined user roles

network-admin

Usage guidelines

CAUTION:

This command might interrupt network communication and cause packet forwarding failure. Before executing the command, make sure you fully understand the potential impact on the network.

When you use this command, the system will prompt you to confirm the operation before deleting all the IPv6 static routes.

Examples

Delete all IPv6 static routes.

```
<Sysname> system-view
[Sysname] delete ipv6 static-routes all
This will erase all IPv6 static routes and their configurations, you must reconfigure all static routes.
Are you sure?[Y/N]:y
```

Related commands

ipv6 route-static

display ipv6 route-static nib

Use **display ipv6 route-static nib** to display IPv6 static route next hop information.

Syntax

display ipv6 route-static nib [*nib-id*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

nib-id: Specifies a NIB by its ID, a hexadecimal string in the range of 1 to ffffffff.

verbose: Displays detailed IPv6 static route next hop information. If you do not specify this keyword, the command displays brief IPv6 static route next hop information.

Examples

Display brief IPv6 static route next hop information.

```
<Sysname> display ipv6 route-static nib
Total number of nexthop(s): 35

      NibID: 0x21000000        Sequence: 0
       Type: 0x41               Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 2::3
    IFIndex: 0x0              LocalAddr: ::
   TopoNthp: Invalid            ExtType: 0x0

      NibID: 0x21000001        Sequence: 1
       Type: 0x41               Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 3::4
    IFIndex: 0x0              LocalAddr: ::
   TopoNthp: Invalid            ExtType: 0x0

...
```

Table 1 Command output

Field	Description
NibID	ID of the NIB.
Sequence	Sequence number of the NIB.
Type	Type of the NIB.
Flushed	Indicates whether the route with the NIB has been flushed to the FIB.
UserKey0	Reserved data 1.
UserKey1	Reserved data 2.
VrfNthp	This field is not supported in the current software version. Index of the VPN instance to which the next hop belongs. This field displays **0** if the next hop is on the public network.
Nexthop	Next hop address.
IFIndex	Interface index
LocalAddr	Local interface address.
TopoNthp	This field is not supported in the current software version. Index of the topology that contains the next hop. This field displays **Invalid** if the next hop is on an IPv6 network, because the router does not support multiple topologies.
ExtType	NIB extension type.

Display detailed IPv6 static route next hop information.

```
<Sysname> display ipv6 route-static nib verbose
```

```
Total number of nexthop(s): 35

      NibID: 0x21000000        Sequence: 0
       Type: 0x41               Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 2::3
    IFIndex: 0x0              LocalAddr: ::
   TopoNthp: Invalid            ExtType: 0x0
     RefCnt: 1              FlushRefCnt: 0
       Flag: 0x12               Version: 1
 1 nexthop(s):
PrefixIndex: 0              OrigNexthop: 2::3
  RelyDepth: 2              RealNexthop: ::
  Interface: NULL0            LocalAddr: ::
  TunnelCnt: 0                      Vrf: default-vrf
   TunnelID: N/A               Topology:
     Weight: 0

      NibID: 0x21000001        Sequence: 1
       Type: 0x41               Flushed: Yes
   UserKey0: 0x0                VrfNthp: 0
   UserKey1: 0x0                Nexthop: 3::4
    IFIndex: 0x0              LocalAddr: ::
   TopoNthp: Invalid            ExtType: 0x0
     RefCnt: 1              FlushRefCnt: 0
       Flag: 0x12               Version: 1
 1 nexthop(s):
PrefixIndex: 0              OrigNexthop: 3::4
  RelyDepth: 1              RealNexthop: ::
  Interface: Vlan11           LocalAddr: ::
  TunnelCnt: 0                      Vrf: default-vrf
   TunnelID: N/A               Topology:
     Weight: 0

...
```

Table 2 Command output

Field	Description
x nexthop(s)	Number of next hops.
PrefixIndex	Prefix index of the next hop for an ECMP route.
Vrf	This field is not supported in the current software version. VPN instance name. For the public network, this field displays **default-vrf**.
OrigNexthop	Original next hop.
RealNexthop	Real next hop.
Interface	Output interface.

Field	Description
localAddr	Local interface address.
RelyDepth	Recursion depth.
TunnelCnt	This field is not supported in the current software version. Number of tunnels after route recursion.
TunnelID	This field is not supported in the current software version. ID of the tunnel after route recursion.
Topology	This field is not supported in the current software version. Topology name. This field is blank for IPv6, because IPv6 does not support multiple topologies.
Weight	ECMP routes are not supported in the current software version. ECMP route weight. This field displays 0 for non-ECMP routes.
RefCnt	Reference count of the next hop.
FlushRefCnt	Reference count of the next hop that is flushed to the FIB.
Flag	Flag of the next hop.
Version	Version of the next hop.
ExtType	NIB extension type.

display ipv6 route-static routing-table

Use **display ipv6 route-static routing-table** to display IPv6 static routing table information.

Syntax

display ipv6 route-static routing-table [*ipv6-address prefix-length*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6-address: Specifies the destination IPv6 address.

prefix-length: Specifies the prefix length in the range of 0 to 128.

Examples

Display IPv6 static routing table information.

```
<Sysname> display ipv6 route-static routing-table
Total number of routes: 5

Status: * - valid

*Destination: 1::1/128
       NibID: 0x21000000        NextHop: 2::2
```

```
   MainNibID: N/A             BkNextHop: N/A
     BkNibID: N/A             Interface: Vlan-interface11
     TableID: 0xa           BkInterface: N/A
        Flag: 0x80d0a          BfdSrcIp: N/A
     DbIndex: 0x3            BfdIfIndex: 0x0
        Type: Normal        BfdVrfIndex: 0
  TrackIndex: 0xffffffff          Label: NULL
  Preference: 60            vrfIndexDst: 0
     BfdMode: N/A            vrfIndexNH: 0
   Permanent: 0                     Tag: 0

*Destination: 1::1234/128
      NibID: 0x21000000        NextHop: 2::2
   MainNibID: N/A             BkNextHop: N/A
     BkNibID: N/A             Interface: NULL0
     TableID: 0xa           BkInterface: N/A
        Flag: 0x80d0a          BfdSrcIp: N/A
     DbIndex: 0x1            BfdIfIndex: 0x0
        Type: Normal        BfdVrfIndex: 0
  TrackIndex: 0xffffffff          Label: NULL
  Preference: 60            vrfIndexDst: 0
     BfdMode: N/A            vrfIndexNH: 0
   Permanent: 0                     Tag: 0

...
```

Table 3 Command output

Field	Description
Destination	Destination address/prefix.
NibID	ID of the NIB.
MainNibID	ID of the primary next hop for static route FRR.
BkNibID	ID of the backup next hop for static route FRR.
NextHop	Next hop address.
BkNextHop	Backup next hop address.
Interface	Output interface of the route.
BkInterface	Backup output interface.
TableID	ID of the table to which the route belongs.
DbIndex	Index of the database to which the route belongs.
Type	Route type: • Normal. • DHCP. • NAT.
BfdSrcIp	Source IPv6 address of the indirect BFD session.
BfdIfIndex	Index of the interface where BFD is enabled.

Field	Description
BfdVrfIndex	This field is not supported in the current software version. Index of the VPN instance where BFD is enabled. This field displays **0** if BFD is enabled for the public network.
BfdMode	BFD session mode: • **N/A**—No BFD session is configured. • **Ctrl**—Control packet mode. • **Echo**—Echo packet mode.
TrackIndex	NQA Track index.
vrfIndexDst	This field is not supported in the current software version. Index of the VPN instance to which the destination belongs. For the public network, this field displays **0**.
vrfIndexNH	This field is not supported in the current software version. Index of the VPN instance to which the next hop belongs. For the public network, this field displays **0**.
Permanent	Permanent static route flag. 1 indicates a permanent static route.

ipv6 route-static

Use **ipv6 route-static** to configure an IPv6 static route.

Use **undo ipv6 route-static** to remove an IPv6 static route.

Syntax

ipv6 route-static *ipv6-address prefix-length* { *interface-type interface-number* [*next-hop-address*] [**bfd** { **control-packet** | **echo-packet** } [**bfd-source** *ipv6-address*] | **permanent**] } [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]

undo ipv6 route-static *ipv6-address prefix-length* [*interface-type interface-number* [*next-hop-address*] | *next-hop-address*] [**preference** *preference*]

Default

No IPv6 static route is configured.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6-address prefix-length: Specifies the IPv6 address and prefix length.

interface-type interface-number: Specifies an output interface by its type and number. If the output interface is an NBMA interface or broadcast interface and not a point-to-point (P2P) interface, the next hop address must be specified.

next-hop-address: Specifies the next hop IPv6 address.

bfd: Enables BFD to detect reachability of the static route's next hop.

control-packet: Specifies the BFD control packet mode.

bfd-source *ipv6-address*: Specifies the source IPv6 address of BFD packets.

echo-packet: Specifies the BFD echo packet mode.

permanent: Specifies the IPv6 route as a permanent IPv6 static route. If the output interface is down, the permanent IPv6 static route is still active.

preference *preference*: Specifies a preference for IPv6 static routes, in the range of 1 to 255. The default is 60.

tag *tag-value*: Sets a tag for marking the static route, in the range of 1 to 4294967295. The default is 0. Tags of routes are used for route control in routing policies. For more information about routing policies, see *Layer 3—IP Routing Configuration Guide*.

description *text*: Configures a description for the IPv6 static route, which consists of 1 to 60 characters, including special characters such as the space, but excluding the question mark (?).

Usage guidelines

An IPv6 static route that has the destination address configured as **::/0** (a prefix length of 0) is the default IPv6 route. If the destination address of an IPv6 packet does not match any entry in the routing table, this default route is used to forward the packet.

Follow these guidelines to configure the output interface, next hop address, or both for a static route:

- If the output interface is a broadcast interface or an NBMA interface, the next hop address must be specified.
- If the output interface is a P2P interface, you can specify only the output interface. You do not need to change the configuration of the route even if the peer address is changed.

Follow these guidelines when you configure BFD for IPv6 static routes:

- If you specify the source IPv6 address of BFD packets, you must specify the IPv6 address as the next hop IPv6 address on the peer device.
- If you specify a non-P2P output interface and a direct next hop, specify the **bfd-source** *ipv6-address* option as a best practice. Make sure the source IPv6 address of BFD packets meets the following requirements:
  - The address is the same as the IPv6 address of the output interface.
  - The address is on the same network segment as the next hop IPv6 address of the same type.

    For example, if the next hop IPv6 address is a link-local address, the source IPv6 address of BFD packets must also be a link-local address.

Follow these guidelines when you configure a static route:

- Enabling BFD for a flapping route could worsen the route flapping situation. Therefore, use it with caution. For more information about BFD, see *High Availability Configuration Guide*.
- The next hop IPv6 address of echo packets must be a global unicast address.
- Do not specify the **permanent** keyword together with the **bfd** keyword.

Examples

Configure an IPv6 static route, with the destination address 1:1:2::/64 and next hop 1:1:3::1.

```
<Sysname> system-view
[Sysname] ipv6 route-static 1:1:2:: 64 1:1:3::1
```

Related commands

display ipv6 routing-table protocol

ipv6 route-static default-preference

Use **ipv6 route-static default-preference** to set a default preference for IPv6 static routes.

Use **undo ipv6 route-static default-preference** to restore the default.

Syntax

ipv6 route-static default-preference *default-preference*

undo ipv6 route-static default-preference

Default

The default preference of IPv6 static routes is 60.

Views

System view

Predefined user roles

network-admin

Parameters

default-preference: Specifies a default preference for IPv6 static routes, in the range of 1 to 255.

Usage guidelines

If no preference is specified for an IPv6 static route, the default preference applies.

When the default preference is reconfigured, it applies only to newly added IPv6 static routes.

Examples

Set a default preference of 120 for IPv6 static routes.

```
<Sysname> system-view
[Sysname] ipv6 route-static default-preference 120
```

Related commands

display ipv6 routing-table protocol

Contents

RIPng commands

The S5000V3-EI, S5000V5-EI, S5000E-X, S5000X-EI, and WAS6000 switch series do not support RIPng.

checkzero

Use **checkzero** to enable zero field check on RIPng packets.

Use **undo checkzero** to disable zero field check.

Syntax

checkzero

undo checkzero

Default

Zero field check is enabled.

Views

RIPng view

Predefined user roles

network-admin

Usage guidelines

Some fields in RIPng packet headers must be zero. These fields are called zero fields. You can enable zero field check on incoming RIPng packets. If a zero field of a packet contains a non-zero value, RIPng discards the packet.

Examples

Disable zero field check on RIPng packets for RIPng 100.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] undo checkzero
```

default cost

Use **default cost** to configure a default metric for redistributed routes.

Use **undo default cost** to restore the default.

Syntax

default cost *cost-value*

undo default cost

Default

The default metric of redistributed routes is 0.

Views

RIPng view

Predefined user roles

network-admin

Parameters

cost-value: Specifies a default metric for redistributed routes, in the range of 0 to 16.

Usage guidelines

When you use the **import-route** command to redistribute routes from another routing protocol without specifying a metric, the metric specified by the **default cost** command applies.

Examples

Configure a default metric of 2 for redistributed routes.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] default cost 2
```

Related commands

import-route

display ripng

Use **display ripng** to display state and configuration information for a RIPng process.

Syntax

display ripng [*process-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays information about all RIPng processes.

Examples

Display state and configuration information for all configured RIPng processes.

```
<Sysname> display ripng
  Public VPN-instance name:

RIPng process: 1
       Preference: 100
           Routing policy: abc
       Checkzero: Enabled
       Default cost: 0
       Maximum number of load balanced routes: 1
       Update time   :   30 secs  Timeout time         :  180 secs
       Suppress time :  120 secs  Garbage-collect time :  120 secs
       Update output delay:   20(ms)  Output count:    3
       Graceful-restart interval:   60 secs
       Triggered Interval : 5 50 200
       Number of periodic updates sent: 256
       Number of triggered updates sent: 0
```

Table 1 Command output

Field	Description
Public VPN-instance name	Public network where the RIPng process runs.
RIPng process	RIPng process ID.
Preference	RIPng preference.
Checkzero	Indicates whether zero field check for RIPng packet headers is enabled: **Enabled** or **Disabled**.
Default Cost	Default metric of redistributed routes.
Maximum number of load balanced routes	ECMP routes are not supported in the current software version. Maximum number of load-balanced routes.
Update time	RIPng update interval, in seconds.
Timeout time	RIPng timeout interval, in seconds.
Suppress time	RIPng suppress interval, in seconds.
Garbage-Collect time	RIPng garbage collection interval, in seconds.
Update output delay	RIPng packet sending interval, in milliseconds.
Output count	Maximum number of RIPng packets that can be sent at each interval.
Graceful-restart interval	GR interval in seconds.
Triggered Interval	Triggered update sending interval.

display ripng database

Use **display ripng database** to display all active routes in the advertising database for a RIPng process.

Syntax

display ripng *process-id* **database** [*ipv6-address prefix-length*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535.

ipv6-address prefix-length: Specifies an IPv6 address. The *ipv6-address* argument specifies an IPv6 address. The *prefix-length* argument specifies a prefix length in the range of 0 to 128.

Examples

Display active routes for RIPng process 1.

```
<Sysname> display ripng 1 database
   1::/64,
```

```
     cost 0, RIPng-interface
  10::/32,
     cost 0, imported
  2::2/128,
    via FE80::20C:29FF:FE7A:E3E4, cost 1
```

Table 2 Command output

Field	Description
cost	Route metric value.
imported	Indicates the route is redistributed from another routing protocol.
RIPng-interface	Route learned from the interface.
via	Next hop IPv6 address.

display ripng graceful-restart

Use **display ripng graceful-restart** to display GR information.

Syntax

display ripng [*process-id*] **graceful-restart**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535.

Examples

Display GR information for RIPng process 1.

```
<Sysname> display ripng 1 graceful-restart
RIPng process: 1
 Graceful Restart capability    : Enabled
 Current GR state               : Normal
 Graceful Restart period        : 60  seconds
 Graceful Restart remaining time: 0   seconds
```

Table 3 Command output

Field	Description
Graceful Restart capability	Indicates whether GR is enabled: **Enabled** or **Disabled**.
Current GR state	GR state: • **Under GR**—GR is in process. • **Normal**—GR is not in progress or has completed.

display ripng interface

Use **display ripng interface** to display interface information for a RIPng process.

Syntax

display ripng *process-id* **interface** [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify this argument, the command displays information about all interfaces for the RIPng process.

Examples

Display interface information for RIPng process 1.

```
<Sysname> display ripng 1 interface
Total: 1

 Interface: Vlan-interface100
        Link-local address: FE80::20C:29FF:FEC8:B4DD
        Split-horizon: On               Poison-reverse: Off
        MetricIn: 0                     MetricOut: 1
        Default route: Off
        Update output delay: 20 (ms)    Output count: 3
        Summary address:
               1::/16
```

Table 4 Command output

Field	Description
Total	Number of interfaces running RIPng.
Interface	Name of an interface running RIPng.
Link Local Address	Link-local address of an interface running RIPng.
Split-horizon	Indicates whether split horizon is enabled: • **On**—Enabled. • **Off**—Disabled.
Poison-reverse	Indicates whether poison reverse is enabled: • **On**—Enabled. • **Off**—Disabled.
MetricIn/MetricOut	Additional metric to incoming and outgoing routes.

Field	Description
Default route	• **Only**—The interface advertises only a default route. • **Originate**—The interface advertises a default route and other RIPng routes. • **Off**—In this state, the interface does not advertise a default route. • **In garbage-collection status**—In this state, the interface advertises a default route with a metric of 16.
Update output delay	RIPng packet sending interval, in milliseconds.
Output count	Maximum number of RIPng packets that an interface can send at each interval.
Default route cost	Cost of the default route.

display ripng neighbor

Use **display ripng neighbor** to display neighbor information for a RIPng process.

Syntax

display ripng *process-id* **neighbor** [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify this argument, the command displays information about all neighbors for the RIPng process.

Examples

Display neighbor information for RIPng process 1.

```
<Sysname> display ripng 1 neighbor
Neighbor Address: FE80::230:FF:FE00:0
     Interface  : Vlan-interface1
     Version    : RIPng version 1     Last update: 00h00m27s
     Bad packets: 0                   Bad routes : 0
```

Table 5 Command output

Field	Description
Neighbor Address	Link-local address of a neighbor interface.
Interface	Name of a neighbor interface.
Version	Version of RIPng that a neighbor runs.
Last update	Time elapsed since the most recent update.

display ripng non-stop-routing

Use **display ripng non-stop-routing** to display RIPng NSR information.

Syntax

display ripng [*process-id*] **non-stop-routing**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535.

Examples

Display NSR information for RIPng process 1.

```
<Sysname> display ripng 1 non-stop-routing
RIPng process: 1
 Nonstop Routing capability: Enabled
 Current NSR state         : Finish
```

Table 6 Command output

Field	Description
Nonstop Routing capability	Indicates whether NSR is enabled: **Enabled** or **Disabled**.
Current NSR state	NSR state: • **Initialization**—Initialization state. • **Smooth**—Upgrading data. • **Advertising**—Advertising routes. • **Redistribution**—Redistributing routes. • **Finish**—Finished.

display ripng route

Use **display ripng route** to display all RIPng routes for a RIPng process.

Syntax

display ripng *process-id* **route** [*ipv6-address prefix-length* [**verbose**] | **peer** *ipv6-address* | **statistics**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535.

ipv6-address prefix-length: Specifies an IPv6 address. The *ipv6-address* argument specifies an IPv6 address. The *prefix-length* argument specifies a prefix length in the range of 0 to 128.

verbose: Displays all routing information for the specified destination IPv6 address. If you do not specify this keyword, the command displays only optimal RIPng routes with the specified destination IPv6 address.

peer *ipv6-address*: Specifies a neighbor by its IPv6 address.

statistics: Displays routing information statistics, including total number of routes and the number of routes learned from each neighbor.

Examples

Display routing information for RIPng process 1.

```
<Sysname> display ripng 1 route
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect, D – Direct
                O - Optimal, F - Flush to RIB
 ------------------------------------------------------------

 Peer FE80::20C:29FF:FED4:7171 on Vlan-interface100
 Destination 4::4/128,
     via FE80::20C:29FF:FED4:7171, cost 1, tag 0, AOF, 5 secs
 Local route
 Destination 3::3/128,
     via ::, cost 0, tag 0, DOF
 Destination 6::/64,
     via ::, cost 0, tag 0, DOF
```

Display information about routes with the specified prefix for RIPng process 1.

```
<Sysname> display ripng 1 route 3::3 128 verbose
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect, D – Direct
                O - Optimal, F - Flush to RIB
 ------------------------------------------------------------
 Peer FE80::4283:59FF:FE97:205 on Vlan-interface100
 Destination 3::3/128,
     via FE80::4283:59FF:FE97:205, cost 1, tag 0, AOF, 28 secs
```

Table 7 Command output

Field	Description
A–Aging	The route is in aging state.
S–Suppressed	The route is in suppressed state.
G–Garbage-collect	The route is in Garbage-collect state.
D–Direct	The route is a direct route.
Local route	The route is a locally generated direct route.
O - Optimal	The route is an optimal route.
F - Flush to RIB	The route has been flushed to the RIB.
Peer	Neighbor connected to the interface.

Field	Description
Destination	IPv6 destination address.
via	Next hop IPv6 address.
cost	Routing metric value.
tag	Route tag.
secs	Time a route entry has stayed in the current state.

Display routing information statistics for RIPng process 1.

```
<Sysname> display ripng 1 route statistics
Peer                                          Optimal/Aging    Garbage
 FE80::20C:29FF:FED4:7171                      1/2              0
 Local                                         2/0              0
 total                                         3/2              0
```

Table 8 Command output

Field	Description
Peer	IPv6 address of the neighbor.
Optimal	Number of optimal routes.
Aging	Number of routes in aging state.
Garbage	Number of routes in Garbage-collection state.
Local	Total number of locally generated direct route.
total	Total number of routes learned from RIPng neighbors.

enable ipsec-profile

Use **enable ipsec-profile** to apply an IPsec profile to a RIPng process.

Use **undo enable ipsec-profile** to remove the IPsec profile from the RIPng process.

Syntax

enable ipsec-profile *profile-name*

undo enable ipsec-profile

Default

No IPsec profile is applied to a RIPng process.

Views

RIPng view

Predefined user roles

network-admin

Parameters

profile-name: Specifies an IPsec profile by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

To configure an IPsec profile, see IPsec in *Security Configuration Guide*.

Examples

Apply IPsec profile **profile001** to RIPng process 1.

```
<Sysname> system-view
[Sysname] ripng 1
[Sysname-ripng-1] enable ipsec-profile profile001
```

fast-reroute

Use **fast-reroute** to configure RIPng FRR.

Use **undo fast-reroute** to disable RIPng FRR.

Syntax

fast-reroute route-policy *route-policy-name*

undo fast-reroute

Default

RIPng FRR is disabled.

Views

RIPng view

Predefined user roles

network-admin

Parameters

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

RIPng FRR is available only when the state of primary link (with Layer 3 interfaces in up state) changes from bidirectional to unidirectional or down.

RIPng FRR is effective only for RIPng routes that are learned from directly connected neighbors.

Examples

Enable RIPng FRR and use routing policy **frr** to specify a backup next hop.

```
<Sysname> system-view
[Sysname] ipv6 prefix-list abc index 10 permit 100:: 64
[Sysname] route-policy frr permit node 10
[Sysname-route-policy-frr-10] if-match ipv6 address prefix-list abc
[Sysname-route-policy-frr-10] apply ipv6 fast-reroute backup-interface vlan-interface 1
backup-nexthop FE80::8
[Sysname-route-policy-frr-10] quit
[Sysname] ripng 100
[Sysname-ripng-100] fast-reroute route-policy frr
```

filter-policy export

Use **filter-policy export** to configure RIPng to filter redistributed routes.

Use **undo filter-policy export** to remove the filtering.

Syntax

filter-policy { *ipv6-acl-number* | **prefix-list** *prefix-list-name* } **export** [*protocol* [*process-id*]]

undo filter-policy export [*protocol* [*process-id*]]

Default

RIPng does not filter redistributed routes.

Views

RIPng view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies an IPv6 ACL by its number in the range of 2000 to 3999 to filter redistributed routes.

prefix-list *prefix-list-name*: Specifies an IPv6 prefix list by its name, a string of 1 to 63 characters, to filter redistributed routes.

protocol: Filters routes redistributed from a routing protocol.

process-id: Specifies the process ID of the specified routing protocol, in the range of 1 to 65535. This argument is available only when the routing protocol is **ripng** or **ospfv3**. The default is 1.

Usage guidelines

If the *protocol* argument is specified, RIPng filters only routes redistributed from the specified routing protocol. Otherwise, RIPng filters all redistributed routes.

To use an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL in one of the following ways:

- To deny/permit a route with the specified destination, use the **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix* command.
- To deny/permit a route with the specified destination and prefix, use the **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix* **destination** *dest dest-prefix* command.

The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the prefix of the route. For the prefix configuration to take effect, specify a contiguous prefix.

Examples

Use IPv6 prefix list to filter redistributed RIPng updates.

```
<Sysname> system-view
[Sysname] ipv6 prefix-list abc index 10 permit 100:1:: 32
[Sysname] ripng 100
[Sysname-ripng-100] filter-policy prefix-list abc export
```

Configure advanced IPv6 ACL 3000 to permit only route 2001::1/128 to pass. Use advanced IPv6 ACL 3000 to filter redistributed routes.

```
<Sysname> system-view
[Sysname] acl ipv6 advanced 3000
[Sysname-acl-ipv6-adv-3000] rule 10 permit ipv6 source 2001::1 128 destination
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff 128
[Sysname-acl-ipv6-adv-3000] rule 100 deny ipv6
[Sysname-acl-ipv6-adv-3000] quit
```

```
[Sysname] ripng 100
[Sysname-ripng-100] filter-policy 3000 export
```

filter-policy import

Use **filter-policy import** to configure RIPng to filter received routes.

Use **undo filter-policy import** to restore the default.

Syntax

filter-policy { *ipv6-acl-number* | **prefix-list** *prefix-list-name* } **import**

undo filter-policy import

Default

RIPng does not filter received routes.

Views

RIPng view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies an IPv6 ACL by its number in the range of 2000 to 3999 to filter received routes.

prefix-list *prefix-list-name*: Specifies an IPv6 prefix list by its name, a string of 1 to 63 characters, to filter received routes.

Usage guidelines

To use an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL in one of the following ways:

- To deny/permit a route with the specified destination, use the **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix* command.
- To deny/permit a route with the specified destination and prefix, use the **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix* **destination** *dest dest-prefix* command.

The **source** keyword specifies the destination address of a route and the **destination** keyword specifies the prefix of the route. For the configuration to take effect, specify a contiguous prefix.

Examples

Use the IPv6 prefix list **abc** to filter received RIPng updates.

```
<Sysname> system-view
[Sysname] ipv6 prefix-list abc index 10 permit 100:1:: 32
[Sysname] ripng 100
[Sysname-ripng-100] filter-policy prefix-list abc import
```

Configure advanced IPv6 ACL 3000 to permit only route 2001::1/128 to pass. Use advanced IPv6 ACL 3000 to filter received routes.

```
<Sysname> system-view
[Sysname] acl ipv6 advanced 3000
[Sysname-acl-ipv6-adv-3000] rule 10 permit ipv6 source 2001::1 128 destination
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff 128
[Sysname-acl-ipv6-adv-3000] rule 100 deny ipv6
```

```
[Sysname-acl-ipv6-adv-3000] quit
[Sysname] ripng 100
[Sysname-ripng-100] filter-policy 3000 import
```

graceful-restart

Use **graceful-restart** to enable Graceful Restart (GR) for RIPng.

Use **undo graceful-restart** to disable RIPng GR.

Syntax

graceful-restart

undo graceful-restart

Default

RIPng GR is disabled.

Views

RIPng view

Predefined user roles

network-admin

Usage guidelines

RIPng GR and RIPng NSR are mutually exclusive. Do not configure the **graceful-restart** command and the **non-stop-routing** command at the same time.

Examples

Enable GR for RIPng process 1.

```
<Sysname> system-view
[Sysname] ripng 1
[Sysname-ripng-1] graceful-restart
```

graceful-restart interval

Use **graceful-restart interval** to set the GR interval.

Use **undo graceful-restart interval** to restore the default.

Syntax

graceful-restart interval *interval*

undo graceful-restart interval

Default

The GR interval is 60 seconds.

Views

RIPng view

Predefined user roles

network-admin

Parameters

interval: Specifies the GR interval in the range of 5 to 360 seconds.

Examples

Set the GR interval to 200 seconds for RIPng process 1.

```
<Sysname> system-view
[Sysname] ripng 1
[Sysname-ripng-1] graceful-restart interval 200
```

import-route

Use **import-route** to redistribute routes from another routing protocol.

Use **undo import-route** to remove routes redistributed from another routing protocol.

Syntax

import-route { **direct** | **static** } [**cost** *cost-value* | **route-policy** *route-policy-name*] *

undo import-route { **direct** | **static** }

import-route { **ospfv3** | **ripng** } [*process-id*] [**allow-direct** | **cost** *cost-value* | **route-policy** *route-policy-name*] *

undo import-route { **ospfv3** | **ripng** } [*process-id*]

Default

RIPng does not redistribute routes from another routing protocol.

Views

RIPng view

Predefined user roles

network-admin

Parameters

direct: Redistributes direct routes.

ospfv3: Redistributes OSPFv3 routes.

ripng: Redistributes RIPng routes.

static: Redistributes static routes.

process-id: Specifies an OSPFv3 or RIPng process by its ID in the range of 1 to 65535. The default is 1.

allow-direct: Redistributes the networks of the local interfaces enabled with the specified routing protocol. If you do not specify this keyword, the networks of the local interfaces are not redistributed. If you specify both the **allow-direct** keyword and the **route-policy** *route-policy-name* option, make sure the **if-match** rule defined in the routing policy does not conflict with the **allow-direct** keyword. For example, if you specify the **allow-direct** keyword, do not configure the **if-match route-type** rule for the routing policy. Otherwise, the **allow-direct** keyword does not take effect.

cost *cost-value*: Specifies a metric for redistributed routes, in the range of 0 to 16. The default metric is 0.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

This command redistributes only active routes. To view route state information, use the **display ipv6 routing-table protocol** command.

Examples

Redistribute routes from OSPFv3process 7 into RIPng and set the metric for redistributed routes to 7.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] import-route ospfv37 cost 7
```

non-stop-routing

Use **non-stop-routing** to enable RIPng NSR.

Use **undo non-stop-routing** to disable RIPng NSR.

Syntax

non-stop-routing

undo non-stop-routing

Default

RIPng NSR is disabled.

Views

RIPng view

Predefined user roles

network-admin

Usage guidelines

RIPng NSR enabled for a RIPng process takes effect only on that process. If multiple RIPng processes exist, enable RIPng NSR for each process as a best practice.

RIPng NSR and RIPng GR are mutually exclusive. Do not configure the **non-stop-routing** command and the **graceful-restart** command at the same time.

Examples

Enable NSR for RIPng process 1.

```
<Sysname> system-view
[Sysname] ripng 1
[Sysname-ripng-1] non-stop-routing
```

output-delay

Use **output-delay** to set the RIPng packet sending interval and the maximum number of RIPng packets that can be sent at each interval.

Use **undo output-delay** to restore the default.

Syntax

output-delay *time* **count** *count*

undo output-delay

Default

A RIPng process sends a maximum of three RIPng packets every 20 milliseconds.

Views

RIPng view

Predefined user roles

network-admin

Parameters

time: Specifies the RIPng packet sending interval in the range of 10 to 100 milliseconds.

count: Specifies the maximum number of RIPng packets sent by a RIPng process at each interval, in the range of 1 to 30.

Usage guidelines

If you configure the RIPng packet sending rate for both a RIPng process and an interface running the RIPng process, the configuration on the interface takes effect.

Examples

Configure RIPng process 1 to send a maximum of 10 RIPng packets every 60 milliseconds.

```
<Sysname> system-view
[Sysname] ripng 1
[Sysname-ripng-1] output-delay 60 count 10
```

Related commands

ripng output-delay

preference

Use **preference** to set the preference for RIPng routes.

Use **undo preference** to restore the default.

Syntax

preference { *preference* | **route-policy** *route-policy-name* } *

undo preference

Default

The preference of RIPng routes is 100.

Views

RIPng view

Predefined user roles

network-admin

Parameters

preference: Specifies the preference for RIPng routes, in the range of 1 to 255. The smaller the value, the higher the preference.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

You can specify a routing policy to set a preference for the matching RIPng routes.

- The preference set by the routing policy applies to all matching RIPng routes. The preference of other routes is set by the **preference** command.
- If no preference is set by the routing policy, the preference of all RIPng routes is set by the **preference** command.

Examples

Set the preference for RIPng routes to 120.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] preference 120
```

reset ripng process

Use **reset ripng process** to restart a RIPng process.

Syntax

reset ripng *process-id* **process**

Views

User view

Predefined user roles

network-admin

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535.

Usage guidelines

After executing the command, you are prompted to confirm the operation.

Examples

Restart RIPng process 100.

```
<Sysname> reset ripng 100 process
Reset RIPng process? [Y/N]:y
```

reset ripng statistics

Use **reset ripng statistics** to clear statistics for a RIPng process.

Syntax

reset ripng *process-id* **statistics**

Views

User view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535.

Examples

Clear statistics for RIPng process 100.

```
<Sysname> reset ripng 100 statistics
```

ripng

Use **ripng** to enable RIPng and enter RIPng view.

Use **undo ripng** to disable RIPng.

Syntax

ripng [*process-id*]

undo ripng [*process-id*]

Default

RIPng is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535. The default value is 1.

Usage guidelines

Before you configure global RIPng parameters, you must create a RIPng process. This restriction does not apply to configuring interface RIPng parameters.

If you disable a RIPng process, the configured RIPng parameters become invalid.

Examples

Create RIPng process 100 and enter its view.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100]
```

ripng default-route

Use **ripng default-route** to configure a RIPng interface to advertise a default route with a specified metric.

Use **undo ripng default-route** to disable a RIPng interface from sending a default route.

Syntax

ripng default-route { **only** | **originate** } [**cost** *cost-value* | **route-policy** *route-policy-name*] *

undo ripng default-route

Default

A RIPng process does not advertise a default route.

Views

Interface view

Predefined user roles

network-admin

Parameters

only: Advertises only an IPv6 default route (::/0).

originate: Advertises an IPv6 default route (::/0) and other routes.

cost-value: Specifies a cost for the default route, in the range of 1 to 15. The default is 1.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters. The command advertises a default route only when a route in the routing table matches the routing policy.

Usage guidelines

This command enables the interface to advertise a RIPng default route in a route update regardless of whether the default route exists in the local IPv6 routing table.

A RIPng interface configured to advertise a default route does not receive any default routes from its neighbors.

Examples

Configure RIPng on VLAN-interface 100 to advertise only a default route.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng default-route only
```

Configure RIPng on VLAN-interface 101 to advertise a default route and other routes.

```
<Sysname> system-view
[Sysname] interface vlan-interface 101
[Sysname-Vlan-interface101] ripng default-route originate
```

ripng enable

Use **ripng enable** to enable RIPng on an interface.

Use **undo ripng enable** to disable RIPng on an interface.

Syntax

ripng *process-id* **enable**

undo ripng enable

Default

RIPng is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

process-id: Specifies a RIPng process by its ID in the range of 1 to 65535.

Examples

Enable RIPng 100 on VLAN-interface 100.

```
<Sysname> system-view
```

```
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng 100 enable
```

ripng ipsec-profile

Use **ripng ipsec-profile** to apply an IPsec profile to a RIPng interface.

Use **undo ripng ipsec-profile** to remove the IPsec profile from the RIPng interface.

Syntax

ripng ipsec-profile *profile-name*

undo ripng ipsec-profile

Default

No IPsec profile is applied to a RIPng interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

profile-name: Specifies an IPsec profile by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

To configure an IPsec profile, see IPsec in *Security Configuration Guide*.

Examples

Apply IPsec profile **profile001** to VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng ipsec-profile profile001
```

ripng metricin

Use **ripng metricin** to configure an interface to add a metric to inbound RIPng routes.

Use **undo ripng metricin** to restore the default.

Syntax

ripng metricin *value*

undo ripng metricin

Default

The additional metric of an inbound route is 0.

Views

Interface view

Predefined user roles

network-admin

Parameters

value: Adds an additional metric to inbound routes, in the range of 0 to 16.

Examples

Configure VLAN-interface 100 to add a metric of 12 to inbound RIPng routes.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng metricin 12
```

ripng metricout

Use **ripng metricout** to configure an interface to add a metric to outbound RIPng routes.

Use **undo ripng metricout** to restore the default.

Syntax

ripng metricout *value*

undo ripng metricout

Default

The additional metric of outbound routes is 1.

Views

Interface view

Predefined user roles

network-admin

Parameters

value: Adds an additional metric to outbound routes, in the range of 1 to 16.

Examples

Configure RIPng on VLAN-interface 100 to add a metric of 12 to outbound routes.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng metricout 12
```

ripng output-delay

Use **ripng output-delay** to set the RIPng packet sending interval and the maximum number of RIPng packets that can be sent by an interface at each interval.

Use **undo ripng output-delay** to restore the default.

Syntax

ripng output-delay *time* **count** *count*

undo ripng output-delay

Default

An interface uses the RIPng packet sending rate set for the RIPng process that the interface runs.

Views

Interface view

Predefined user roles

network-admin

Parameters

time: Specifies the RIPng packet sending interval in the range of 10 to 100 milliseconds.

count: Specifies the maximum number of RIPng packets sent at each interval, in the range of 1 to 30.

Usage guidelines

If you set the RIPng packet sending rate for both a RIPng process and an interface running the RIPng process, the configuration on the interface takes effect.

Examples

Configure VLAN-interface 100 to send a maximum of six RIPng packets every 30 milliseconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng output-delay 30 count 6
```

Related commands

output-delay

ripng poison-reverse

Use **ripng poison-reverse** to enable poison reverse.

Use **undo ripng poison-reverse** to disable poison reverse.

Syntax

ripng poison-reverse

undo ripng poison-reverse

Default

Poison reverse is disabled.

Views

Interface view

Predefined user roles

network-admin

Examples

Enable poison reverse for RIPng update messages on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng poison-reverse
```

ripng primary-path-detect bfd echo

Use **ripng primary-path-detect bfd echo** to enable BFD single-hop echo detection for RIPng FRR.

Use **undo ripng primary-path-detect bfd** to disable BFD single-hop echo detection for RIPng FRR.

Syntax

ripng primary-path-detect bfd echo

undo ripng primary-path-detect bfd

Default

BFD single-hop echo detection is disabled for RIPng FRR.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

For quicker RIPng FRR, use BFD single-hop echo detection on the primary link of redundant links to detect link failure.

Examples

Enable BFD single-hop echo detection for RIPng FRR on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] ripng 1
[Sysname-ripng-1] fast-reroute route-policy frr
[Sysname-ripng-1] quit
[Sysname] bfd echo-source-ipv6 1::1
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ripng primary-path-detect bfd echo
```

ripng split-horizon

Use **ripng split-horizon** to enable split horizon.

Use **undo ripng split-horizon** to disable split horizon.

Syntax

ripng split-horizon

undo ripng split-horizon

Default

Split horizon is enabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

Split horizon prevents routing loops. If you want to disable this feature, make sure the operation is indispensable.

If both poison reverse and split horizon are enabled, only poison reverse takes effect.

Examples

Enable split horizon on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng split-horizon
```

ripng summary-address

Use **ripng summary-address** to configure a summary network to be advertised through an interface.

Use **undo ripng summary-address** to remove a summary network.

Syntax

ripng summary-address *ipv6-address prefix-length*

undo ripng summary-address *ipv6-address prefix-length*

Default

No summary network is configured to be advertised through an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the destination IPv6 address of the summary route.

prefix-length: Specifies the prefix length of the destination IPv6 address of the summary route, in the range of 0 to 128. It indicates the number of consecutive 1s of the prefix, which defines the network ID.

Usage guidelines

Networks on the summary network will not be advertised. The cost of the summary route is the lowest cost among summarized routes.

Examples

Assign an IPv6 address with the 64-bit prefix to VLAN-interface 100 and configure a summary with the 35-bit prefix.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001:200::3EFF:FE11:6770/64
[Sysname-Vlan-interface100] ripng summary-address 2001:200:: 35
```

timer triggered

Use **timer triggered** to set the interval for sending triggered updates.

Use **undo timer triggered** to restore the default.

Syntax

timer triggered *maximum-interval* [*minimum-interval* [*incremental-interval*]]

undo timer triggered

Default

The maximum, minimum, and incremental intervals for sending triggered updates are 5 seconds, 50 milliseconds, and 200 milliseconds, respectively.

Views

RIPng view

Predefines user roles

network-admin

Parameters

maximum-interval: Specifies the maximum interval for sending triggered updates, in the range of 1 to 5 seconds.

minimum-interval: Specifies the minimum interval for sending triggered updates, in the range of 10 to 5000 milliseconds.

incremental-interval: Specifies the incremental interval for sending triggered updates, in the range of 100 to 1000 milliseconds.

Usage guidelines

The minimum interval and the incremental interval cannot be greater than the maximum interval.

For a stable network, the minimum interval is used. If network changes become frequent, the incremental interval *incremental-interval* is used to increase the triggered update sending interval until the *maximum-interval* is reached.

Examples

Set the maximum, minimum, and incremental intervals for sending triggered updates to 2 seconds, 100 milliseconds, and 100 milliseconds, respectively.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] timer triggered 2 100 100
```

timers

Use **timers** to set RIPng timers.

Use **undo timers** to restore the default.

Syntax

timers { **garbage-collect** *garbage-collect-value* | **suppress** *suppress-value* | **timeout** *timeout-value* | **update** *update-value* } *

undo timers { **garbage-collect** | **suppress** | **timeout** | **update** } *

Default

The garbage-collect timer is 120 seconds, the suppress timer is 120 seconds, the timeout timer is 180 seconds, and the update timer is 30 seconds.

Views

RIPng view

Predefines user roles

network-admin

Parameters

garbage-collect-value: Sets the garbage-collect timer in the range of 1 to 86400 seconds.

suppress-value: Sets the suppress timer in the range of 0 to 86400 seconds.

timeout-value: Sets the timeout timer in the range of 1 to 86400 seconds.

update-value: Sets the update timer in the range of 1 to 86400 seconds.

Usage guidelines

RIPng has the following timers:

- **Update timer**—Interval between update messages.
- **Timeout timer**—Route aging time. If no update for a route is received before the timer expires, RIPng sets the metric of the route to 16.
- **Suppress timer**—How long a RIPng route stays in suppressed state. When the metric of a route becomes 16, the route enters the suppressed state. If RIPng receives an update for the route from the same neighbor and the route in the update has a metric less than 16, RIPng uses the route to replace the suppressed route.
- **Garbage-collect timer**—Interval from when the metric of a route becomes 16 to when it is deleted from the routing table. During the garbage-collect timer length, RIPng advertises the route with a metric of 16. If no update is announced for that route before the garbage-collect timer expires, RIPng deletes the route from the routing table.

As a best practice, do not change the default values of these timers.

The timer lengths must be kept consistent on all routers in the network.

Examples

Set the update, timeout, suppress, and garbage-collect timers to 5 seconds, 15 seconds, 15 seconds, and 30 seconds.

```
<Sysname> system-view
[Sysname] ripng 1
[Sysname-ripng-1] timers update 5 timeout 15 suppress 15 garbage-collect 30
```

Contents

OSPFv3 commands

The S5110V2-SI, S5000V3-EI, S5000V5-EI, S5000E-X, S5000X-EI, and WAS6000 switch series do not support OSPFv3.

abr-summary (OSPFv3 area view)

Use **abr-summary** to configure route summarization on an ABR.

Use **undo abr-summary** to remove the configuration.

Syntax

abr-summary *ipv6-address prefix-length* [**not-advertise**] [**cost** *cost-value*]

undo abr-summary *ipv6-address prefix-length*

Default

Route summarization is not configured on an ABR.

Views

OSPFv3 area view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the destination IPv6 address of the summary route.

prefix-length: Specifies the prefix length of the destination IPv6 address, in the range of 0 to 128. This argument specifies the number of consecutive 1s of the prefix, which defines the network ID.

not-advertise: Specifies not to advertise the summary IPv6 route. If you do not specify this keyword, the command advertises the IPv6 summary route.

cost *cost-value*: Specifies the cost of the summary route, in the range of 1 to 16777215. The default cost is the largest cost value among routes that are summarized.

Usage guidelines

This command applies only to an ABR to summarize multiple contiguous networks into one network.

To enable ABR to advertise specific routes that have been summarized, use the **undo abr-summary** command.

Examples

Summarize networks 2000:1:1:1::/64 and 2000:1:1:2::/64 in Area 1 into 2000:1:1::/48.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 1
[Sysname-ospfv3-1-area-0.0.0.1] abr-summary 2000:1:1:: 48
```

area

Use **area** to create an OSPFv3 area and enter OSPFv3 area view.

Use **undo area** to remove an OSPFv3 area.

Syntax

area *area-id*

undo area *area-id*

Default

No OSPFv3 areas exist.

Views

OSPFv3 view

Predefined user roles

network-admin

Parameters

area-id: Specifies an area by its ID, an IPv4 address or a decimal integer in the range of 0 to 4294967295 that is translated into the IPv4 address format.

Examples

Create OSPFv3 Area 0 and enter its view.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 0
[Sysname-ospfv3-1-area-0.0.0.0]
```

asbr-summary (OSPFv3 view)

Use **asbr-summary** to configure route summarization on an ASBR.

Use **undo asbr-summary** to remove the configuration.

Syntax

asbr-summary *ipv6-address prefix-length* [**cost** *cost-value* | **not-advertise** | **nssa-only** | **tag** *tag*] *

undo asbr-summary *ipv6-address prefix-length*

Default

Route summarization is not configured on an ASBR.

Views

OSPFv3 view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the destination IPv6 address of the summary route.

prefix-length: Specifies the prefix length in the range of 0 to 128.

cost *cost-value*: Specifies the cost of the summary route, in the range of 1 to 16777214. If you do not specify this option, the largest cost among the summarized routes applies. If the routes in Type-5 LSAs translated from Type-7 LSAs are Type-2 external routes, the largest cost among the summarized routes plus 1 applies.

not-advertise: Disables advertising the summary route. If you do not specify this keyword, the command advertises the route.

nssa-only: Limits the route advertisement to the NSSA area by setting the P-bit of Type-7 LSAs to 0. By default, the P-bit of Type-7 LSAs is set to 1. If the ASBR is also an ABR and **FULL** state neighbors exist in the backbone area, the P-bit of Type-7 LSAs originated by the ASBR is set to 0. This keyword applies to the NSSA ASBR.

tag *tag*: Specifies a tag for the summary route, in the range of 0 to 4294967295.

Usage guidelines

An ASBR can summarize routes in the following LSAs:

- Type-5 LSAs.
- Type-7 LSAs in an NSSA area.
- Type-5 LSAs translated by the ASBR (also an ABR) from Type-7 LSAs in an NSSA area.

  If the ASBR (ABR) is not a translator, it cannot summarize routes in Type-5 LSAs translated from Type-7 LSAs.

To enable ASBR to advertise specific routes that have been summarized, use the **undo asbr-summary** command.

Examples

Configure a summary route 2000::/16, and specify a cost of 100 and a tag value of 2 for the summary route.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] asbr-summary 2000:: 16 cost 100 tag 2
```

authentication-mode

Use **authentication-mode** to specify an authentication mode for an OSPFv3 area.

Use **undo authentication-mode** to restore the default.

Syntax

authentication-mode keychain *keychain-name*

undo authentication-mode

Default

No authentication is performed for an area.

Views

OSPFv3 area view

Predefined user roles

network-admin

Parameters

keychain: Specifies the keychain authentication mode.

keychain-name: Specifies a keychain by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

The authentication mode specified for an OSPFv3 interface has a higher priority than the mode specified for an OSPFv3 area.

When keychain authentication is configured for an OSPFv3 area, OSPFv3 performs the following operations before sending a packet:

1. Obtains a valid send key from the keychain.

   OSPFv3 does not send the packet if it fails to obtain a valid send key.
2. Uses the key ID, authentication algorithm, and key string to authenticate the packet.

   If the key ID is greater than 65535, OSPFv3 does not send the packet.

When keychain authentication is configured for an OSPFv3 area, OSPFv3 performs the following operations after receiving a packet:

1. Uses the key ID carried in the packet to obtain a valid accept key from the keychain.

   OSPFv3 discards the packet if it fails to obtain a valid accept key.
2. Uses the authentication algorithm and key string for the valid accept key to authenticate the packet.

   If the authentication fails, OSPFv3 discards the packet.

OSPFv3 supports only the HMAC-SHA-256 authentication algorithms.

The ID of keys used for authentication can only be in the range of 0 to 65535.

Examples

Configure OSPFv3 Area 1 to use keychain **test** for packet authentication.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 1
[Sysname-ospfv3-1-area-0.0.0.1] authentication-mode keychain test
```

bandwidth-reference (OSPFv3 view)

Use **bandwidth-reference** to set a reference bandwidth value for link cost calculation.

Use **undo bandwidth-reference** to restore the default.

Syntax

bandwidth-reference *value*

undo bandwidth-reference

Default

The reference bandwidth value is 100 Mbps for link cost calculation.

Views

OSPFv3 view

Predefined user roles

network-admin

Parameters

value: Specifies the reference bandwidth value for link cost calculation, in the range of 1 to 4294967 Mbps.

Usage guidelines

You can configure an OSPFv3 cost for an interface with one of the following methods:

- Configure the cost value in interface view.

- Configure a bandwidth reference value. OSPFv3 computes the cost automatically based on the bandwidth reference value by using the following formula: Interface OSPFv3 cost = Bandwidth reference value / Interface bandwidth.
  - If the calculated cost is greater than 65535, the value of 65535 is used.
  - If the calculated cost is smaller than 1, the value of 1 is used.

If no cost value is configured for an interface, OSPFv3 computes the interface cost value automatically.

Examples

Set the reference bandwidth value to 1000 Mbps.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] bandwidth-reference 1000
```

default tag

Use **default tag** to set a tag for redistributed routes.

Use **undo default tag** to restore the default.

Syntax

default tag *tag*

undo default tag

Default

The tag of redistributed routes is 1.

Views

OSPFv3 view

Predefined user roles

network-admin

Parameters

tag: Specifies a tag for redistributed routes, in the range of 0 to 4294967295.

Usage guidelines

If you do not set a tag for redistributed routes by using the **default-route-advertise** or **import-route** command, the tag specified by the **default tag** command applies.

Examples

Set the tag for redistributed routes to 2.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] default tag 2
```

Related commands

default-route-advertise (OSPFv3 view)

import-route

default-cost (OSPFv3 area view)

Use **default-cost** to set a cost for the default route advertised to the stub area or NSSA area.

Use **undo default-cost** to restore the default.

Syntax

default-cost *cost*

undo default-cost

Default

The cost is 1.

Views

OSPFv3 area view

Predefined user roles

network-admin

Parameters

value: Specifies a cost for the default route advertised to the stub area or NSSA area, in the range of 0 to 16777214.

Usage guidelines

This command takes effect only on the ABR of a stub area or the ABR or ASBR of an NSSA area.

Examples

Configure Area 1 as a stub area, and set the cost of the default route advertised to the stub area to 60.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 1
[Sysname-ospfv3-1-area-0.0.0.1] stub
[Sysname-ospfv3-1-area-0.0.0.1] default-cost 60
```

Related commands

nssa (OSPFv3 area view)

stub (OSPFv3 area view)

default-route-advertise (OSPFv3 view)

Use **default-route-advertise** to redistribute a default route into the OSPFv3 routing domain.

Use **undo default-route-advertise** to restore the default.

Syntax

default-route-advertise [[**always** | **permit-calculate-other**] | **cost** *cost-value* | **route-policy** *route-policy-name* | **tag** *tag* | **type** *type*] *

undo default-route-advertise

Default

No default route is redistributed into the OSPFv3 routing domain.

Views

OSPFv3 view

Predefined user roles

network-admin

Parameters

always: Redistributes a default route in an AS-external-LSA into the OSPFv3 routing domain regardless of whether a default route exists in the routing table. If you do not specify this keyword, the router redistributes a default route in an AS-external-LSA into the OSPFv3 routing domain only when the default route exists in the routing table.

permit-calculate-other: Enables OSPFv3 to calculate default routes received from other routers. If you do not specify this keyword, OSPFv3 does not calculate default routes from other routers. If the router does not redistribute any default route in an AS-external-LSA into the OSPFv3 routing domain, the router calculates default routes from other routers. It calculates these routes regardless of whether this keyword is specified.

cost *cost-value*: Specifies a cost for the default route, in the range of 0 to 16777214. The default is 1.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters. When the routing policy is matched and one of the following conditions is met, the command redistributes a default route in an AS-external-LSA into the OSPFv3 routing domain:

- A default route exists in the routing table.
- The **always** keyword is specified.

The routing policy modifies values in the AS-external-LSA.

tag *tag*: Specifies a tag for the default route, in the range of 0 to 4294967295. If you do not specify this option, the tag specified by the **default tag** command applies.

type *type*: Specifies a type for the AS-external-LSA, 1 or 2. The default is 2.

Usage guidelines

This command redistributes a default route in an AS-external-LSA, which cannot be redistributed with the **import-route** command. If the local routing table has no default route, you must provide the **always** keyword for the command.

Examples

Redistribute a default route into the OSPFv3 routing domain. (The default route does not exist in the local router.)

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] default-route-advertise always
```

Related commands

import-route (OSPFv3 view)

display ospfv3

Use **display ospfv3** to display OSPFv3 process information.

Syntax

display ospfv3 [*process-id*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays information about all OSPFv3 processes.

verbose: Displays detailed OSPFv3 process information. If you do not specify this keyword, the command displays brief OSPFv3 process information.

Examples

Display detailed information about all OSPFv3 processes.

```
<Sysname> display ospfv3 verbose

               OSPFv3 Process 1 with Router ID 1.1.1.1

 RouterID: 1.1.1.1          Router type:  ABR  ASBR  NSSA
 Route tag: 0
 Route tag check: Disabled
 Multi-VPN-Instance: Disabled
 Type value of extended community attributes:
    Domain ID : 0x0005
    Route type: 0x0306
    Router ID : 0x0107
 Domain-id: 0.0.0.0
 DN-bit check: Enabled
 DN-bit set: Enabled
 Originating router-LSAs with maximum metric
    Condition: On startup for 600 seconds, State: Inactive
    Advertise summary-LSAs with metric 16711680
    Advertise external-LSAs with metric 16711680
    Advertise intra-area-prefix-LSAs with maximum metric
 SPF-schedule-interval: 5 50 200
 LSA generation interval: 5
 LSA arrival interval: 1000
 Transmit pacing: Interval: 20 Count: 3
 Default ASE parameters: Tag: 1
 Route preference: 10
 ASE route preference: 150
 FRR backup mode: LFA
 SPF calculation count: 0
 External LSA count: 0
 LSA originated count: 0
 LSA received count: 0
 SNMP trap rate limit interval: 10  Count: 7
 Area count: 2  Stub area count: 0  NSSA area count: 1
```

```
ExChange/Loading neighbors: 0
Max equal cost paths: 32
Up interfaces: 1
Full neighbors: 1
Normal areas with up interfaces: 1
Calculation trigger type: Full
Current calculation type: SPF calculation
Current calculation phase: Calculation area topology
Redistribute timer: Off
Redistribute schedule type: RIB
Redistribute route count: 0
Process reset state: N/A
Current reset type: N/A
Next reset type: N/A
Reset prepare message replied: -/-/-/-
Reset process message replied: -/-/-/-
Reset phase of module:
  M-N/A, P-N/A, S-N/A, C-N/A, R-N/A

Area: 0.0.0.0
Area flag: Normal
SPF scheduled count: 0
ExChange/Loading neighbors: 0
LSA count: 0
Up interfaces: 0
MTU: 1440
Default cost: 1
Created by Vlink
Process reset state: N/A
Current reset type: N/A
Reset prepare message replied: -/-/-/-
Reset process message replied: -/-/-/-
Reset phase of module:
  M-N/A, P-N/A, S-N/A, C-N/A, R-N/A

Area: 0.0.0.2
Area flag: Normal
SPF scheduled count: 0
ExChange/Loading neighbors: 0
LSA count: 0
IPsec profile name: Profile000
Keychain authentication: Enabled (test)
Up interfaces: 1
MTU: 1500
Default cost: 1
Process reset state: N/A
Current reset type: N/A
Reset prepare message replied: -/-/-/-
```

```
Reset process message replied: -/-/-/-
Reset phase of module:
  M-N/A, P-N/A, S-N/A, C-N/A, R-N/A

Area: 0.0.0.3
Area flag: NSSA
7/5 translator state: Disabled
7/5 translate stability timer interval: 0
SPF Scheduled Count: 0
ExChange/Loading neighbors: 0
LSA Count: 0
Up interfaces: 0
MTU: 1440
Default cost: 1
Process reset flag: N/A
Current reset type: N/A
Reset prepare message replied: -/-/-/-
Reset process message replied: -/-/-/-
Reset phase of module:
  M-N/A, P-N/A, S-N/A, C-N/A, R-N/A
```

Table 1 Command output

Field	Description
OSPFv3 Process 1 with Router ID 1.1.1.1	OSPFv3 process is 1, and router ID is 1.1.1.1.
Router type	Router type: • ABR. • ASBR. • NSSA. • Null.
Route tag	Tag of the routes redistributed into the OSPFv3 process.
Route tag check	Whether the check is enabled for the route tag in OSPFv3 LSAs of the OSPFv3 process.
Multi-VPN-Instance	Whether the OSPFv3 process supports multiple VPN instances: • **Multi-VPN-Instance: Disabled**—The process does not support multiple VPN instances. • **Multi-VPN-Instance: Enabled**—The process supports multiple VPN instances.
DN-bit check	Whether the check is enabled for the DN bit in OSPFv3 LSAs of the OSPFv3 process.
DN-bit set	Whether the DN bit is set for OSPFv3 LSAs in the OSPFv3 process.
Condition	Time when the router acts as a stub router: • Always. • On startup for *xxx* seconds, where *xxx* is specified by the user.

Field	Description
State	State of the stub router: • Active. • Inactive.
SPF-schedule-interval	Interval for SPF calculations.
Transmit pacing	LSU advertisement rate: • **Interval**—Specifies the interval for sending LSUs. • **Count**—Specifies the maximum number of LSUs sent at each interval.
Default ASE parameters	Default parameters of redistributed routes. **Tag** represents the route tag of the redistributed routes.
Route preference	Internal route preference.
ASE route preference	AS-external route preference.
FRR backup mode	FRR backup mode: • **LFA**—Uses the LFA algorithm to calculate a backup next hop for all routes. **LFA ABR-only** indicates that only the next hop of the route to the ABR can be used as the backup next hop. • **route-policy** *route-policy-name*—Specifies a backup next hop by using a routing policy.
LSA originated count	Number of originated LSAs.
LSA received count	Number of received LSAs.
SNMP trap rate limit interval: 10 Count: 7	The OSPFv3 process can output a maximum of seven notifications within 10 seconds.
Area count	Total number of areas.
Stub area count	Number of stub areas.
NSSA area count	Number of NSSA areas.
ExChange/Loading neighbors	Neighbors in ExChange/Loading state.
Calculation trigger type	Route calculation trigger type: • **Full**—Calculation of all routes is triggered. • **Area topology change**—Topology change in an area. • **Intra router change**—Incremental intra-area route change. • **ASBR change**—Incremental ASBR route change. • **Full IP prefix**—Calculation of all IP prefixes is triggered. • **Full intra AS**—Calculation of all intra-AS prefixes is triggered. • **Inc intra AS**—Calculation of incremental intra-AS prefixes is triggered. • **Full inter AS**—Calculation of all AS-external prefixes is triggered. • **Inc inter AS**—Calculation of incremental AS-external prefixes is triggered. • **Nexthop calculation**—Calculation of next hops is triggered. • **N/A**—Route calculation is not triggered.

Field	Description
Current calculation type	Current route calculation type: • SPF calculation. • **Intra router calculation**—Intra-area route calculation. • **ASBR calculation**—Inter-area ASBR route calculation. • **Inc intra router**—Incremental intra-area route calculation. • **Inc ASBR calculation**—Incremental inter-area ASBR route calculation. • **Full intra AS**—Calculation of all intra-AS prefixes. • **Inc intra AS**—Calculation of incremental intra-AS prefixes. • **Full inter AS**—Calculation of all AS-external prefixes. • **Inc inter AS**—Calculation of incremental AS-external prefixes. • **N/A**—Route calculation is not triggered.
Current calculation phase	Current route calculation phase: • **Calculation area topology**—Calculating area topology. • **Calculation router**—Calculating routes on routers. • **Calculation intra AS**—Calculating intra-AS routes. • **Calculation ASBR**—Calculating routes on ASBRs. • **Calculation inter AS**—Calculating AS-external routes. • **Calculation end**—Ending phase of calculation. • **N/A**—Route calculation is not triggered.
Redistribute timer	Route redistribution timer status: on or off.
Redistribute schedule type	Route redistribution scheduling type: • **RIB**—Redistribute routes through the RIB table. • **Self**—Redistribute routes through the routing table. • **N/A**—Route redistribution is not triggered.
Redistribute route count	Number of redistributed routes.
Process reset state	Process reset state: • **N/A**—The process is not reset. • **Under reset**—The process is in the reset progress. • **Under RIB smooth**—The process is synchronizing RIB routes.
Current reset type	Current process reset type: • **N/A**—The process is not reset. • **GR quit**—Normal reset when GR quits abnormally. • **Delete**—Delete OSPFv3 process. • **Undo router-id**—Delete router ID. • **Set router-id**—Set router ID.
Next reset type	Next process reset type: • **N/A**—The process is not reset. • **GR quit**—Normal reset when GR quits abnormally. • **Delete**—Delete OSPFv3 process. • **Undo router-id**—Delete router ID. • **Set router-id**—Set router ID.

Field	Description
Reset prepare message replied	Modules that reply reset prepare messages: • **P**—Neighbor maintenance module. • **S**—LSDB synchronization module. • **C**—Route calculation module. • **R**—Route redistribution module.
Reset process message replied	Modules that reply reset process messages: • **P**—Neighbor maintenance module. • **S**—LSDB synchronization module. • **C**—Route calculation module. • **R**—Route redistribution module.

Reset phase of module	Reset phase of each module:
	• LSDB synchronization (S) module:
	  ○ **N/A**—Not reset.
	  ○ **Delete ASE**—Delete all ASE LSAs.
	  ○ **Delete area LSA**—Delete LSAs from an area.
	  ○ **Delete area IF**—Delete interfaces from an area.
	• Route calculation (C) module:
	  ○ **N/A**—Not reset.
	  ○ **Delete topology**—Delete area topology.
	  ○ **Delete router**—Delete routes of routers.
	  ○ **Delete intra AS**—Delete intra-AS routes
	  ○ **Delete inter AS**—Delete AS-external routes.
	  ○ **Delete ASBR**—Delete ASBR routes.
	• Route redistribution (R) module:
	  ○ **N/A**—Not reset.
	  ○ **Delete import**—Delete redistributed routes.

IPsec profile name	IPsec profile applied to the interface.
Keychain authentication: Enabled (test)	Keychain authentication is enabled for the area, and the keychain **test** is used.
Created by Vlink	The area is created through virtual link.
7/5 translator state	State of the translator that translates Type-7 LSAs to Type-5 LSAs: • **Enabled**—The translator is specified through commands. • **Elected**—The translator is designated through election. • **Disabled**—The device is not a translator.
7/5 translate stability timer interval	Stability interval (in seconds) for Type-7 LSA-to-Type-5 LSA translation.

display ospfv3 abr-asbr

Use **`display ospfv3 abr-asbr`** to display information about the routes to OSPFv3 ABR and ASBR.

Syntax

`display ospfv3` [*`process-id`*] **`abr-asbr`**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays information about all the routes to the OSPFv3 ABR and ASBR.

Examples

Display information about all the routes to the OSPFv3 ABR and ASBR.

```
<Sysname> display ospfv3 abr-asbr

              OSPFv3 Process 1 with Router ID 1.1.1.1

 Destination : 1.1.1.2                                 Rtr Type : ABR
 Area        : 0.0.0.0                                 Path Type: Intra
 Interface   : Vlan102                               BkInterface: Vlan101
 NextHop     : FE80:1:1::1
 BkNexthop   : FE80:1:2::2
 Cost        : 1

 Destination : 1.1.1.3                                 Rtr Type : ASBR
 Area        : 0.0.0.0                                 Path Type: Intra
 Interface   : Vlan103                               BkInterface: Vlan104
 NextHop     : FE80:2:1::1
 BkNexthop   : FE80:1:2::4
 Cost        : 1
```

Table 2 Command output

Field	Description
OSPFv3 Process 1 with Router ID 1.1.1.1	OSPFv3 process is 1, and router ID is 1.1.1.1.
Destination	Router ID of an ABR or ASBR.
Rtr Type	Router type: ABR or ASBR.
Area	Area ID of the next hop.
Path Type	Type of the route to the ABR or ASBR: • **Intra**—Intra-area route. • **Inter**—Inter-area route.
Interface	Output interface.
NextHop	Next hop address.
BkInterface	Backup output interface.
BkNexthop	Backup next hop address.
Cost	Cost from the router to the ABR or ASBR.

display ospfv3 abr-summary

Use **display ospfv3 abr-summary** to display ABR summary route information.

Syntax

display ospfv3 [*process-id*] [**area** *area-id*] **abr-summary** [*ipv6-address prefix-length*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays information about ABR summary routes for all OSPFv3 processes.

area *area-id*: Specifies an OSPFv3 area by its ID. The area ID is an IP address or a decimal integer in the range of 0 to 4294967295 that is translated into the IP address format. If you do not specify this option, the command displays information about ABR summary routes for all OSPFv3 areas.

ipv6-address prefix-length: Specifies an IPv6 address. The *ipv6-address* argument specifies an IPv6 prefix. The *prefix-length* argument specifies a prefix length in the range of 0 to 128. If you do not specify this argument, the command displays information about all summary routes on the ABR.

verbose: Displays detailed ABR summary route information. If you do not specify this keyword, the command displays brief ABR summary route information.

Examples

Display brief ABR summary route information in OSPFv3 process 1.

```
<Sysname> display ospfv3 1 abr-summary

            OSPFv3 Process 1 with Router ID 2.2.2.2

                    Area: 1.1.1.1
 Total summary addresses: 1

 Prefix      : 1000:4::/32
 Status      : Advertise
 NULL0       : Active
 Cost        : 1 (Configured)
 Routes count: 2
```

Table 3 Command output

Field	Description
Area	Area to which the summary routes belong.
Total summary addresses	Total number of summary routes.
Prefix	Prefix of the summary route.

Field	Description
Status	Advertisement status of the summary route.
NULL0	Null 0 route.
Cost	Cost of the summary route.
Routes count	Number of summarized routes.

Display detailed ABR summary route information in OSPFv3 process 1.

```
<Sysname> display ospfv3 1 abr-summary verbose

            OSPFv3 Process 1 with Router ID 2.2.2.2

                       Area: 1.1.1.1
Total summary addresses: 1

 Prefix      : 1000:4::/32
 Status      : Advertise
 NULL0       : Active
 Cost        : 1 (Configured)
 Routes count: 2
   Destination                                    Metric
   1000:4:10:3::/96                               1
   1000:4:11:3::/96                               1
```

Table 4 Command output

Field	Description
Destination	Destination address of a summarized route.
Metric	Metric of a summarized route.

display ospfv3 asbr-summary

Use **display ospfv3 asbr-summary** to display ASBR summary route information.

Syntax

display ospfv3 [*process-id*] **asbr-summary** [*ipv6-address prefix-length*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays information about ASBR summary routes for all OSPFv3 processes.

ipv6-address prefix-length: Specifies an IPv6 address. The *ipv6-address* argument specifies an IPv6 prefix. The *prefix-length* argument specifies a prefix length in the range of 0 to 128. If you do not specify this argument, the command displays information about all ASBR summary routes.

verbose: Displays detailed ASBR summary route information. If you do not specify this keyword, the command displays brief ASBR summary route information.

Examples

Display brief ASBR summary route information in OSPFv3 process 1.

```
<Sysname> display ospfv3 1 asbr-summary

              OSPFv3 Process 1 with Router ID 2.2.2.2

 Total summary addresses: 1

 Prefix      : 1000:4::/32
 Status      : Advertise
 NULL0       : Active
 Cost        : 1 (Configured)
 Tag         : (Not configured)
 Nssa-only   : (Not configured)
 Routes count: 2
```

Table 5 Command output

Field	Description
Total summary addresses	Total number of summary routes.
Prefix	Prefix and prefix length of the summary route.
Status	Advertisement status of the summary route: • **Advertise**—The summary route has been advertised. • **Not-advertise**—The summary route has not been advertised.
NULL0	Status of the Null 0 route: • Active. • Inactive.
Cost	Cost of the summary route: • Configured. • Not configured.
Tag	Tag of the summary route: • Configured. • Not configured.
Nssa-only	Whether the **nssa-only** attribute is configured: • Configured. • Not configured.
Routes count	Number of summarized routes.

Display detailed ASBR summary route information in OSPFv3 process 1.

```
<Sysname> display ospfv3 1 asbr-summary verbose
```

```
              OSPFv3 Process 1 with Router ID 2.2.2.2

 Total summary addresses: 1

 Prefix      : 1000:4::/32
 Status      : Advertise
 NULL0       : Active
 Cost        : 1 (Configured)
 Tag         : (Not configured)
 Nssa-only   : (Not configured)
 Routes count: 2
  Destination                                Protocol Process Type Metric
  1000:4:10:3::/96                           Static   0       2    1
  1000:4:11:3::/96                           Static   0       2    1
```

Table 6 Command output

Field	Description
Destination	Prefix and prefix length of the summarized route.
Protocol	Routing protocol from which the route was redistributed.
Process	Process of the routing protocol from which the route was redistributed.
Type	Type of the summarized route.
Metric	Metric of the summarized route.

display ospfv3 event-log

Use **display ospfv3 event-log** to display OSPFv3 log information.

Syntax

display ospfv3 [*process-id*] **event-log** { **lsa-flush** | **peer** | **spf** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays OSPFv3 log information for all processes.

lsa-flush: Specifies LSA aging log information.

peer: Specifies neighbor log information.

spf: Specifies route calculation log information.

Usage guidelines

Route calculation logs show the number of routes newly installed in the IPv6 routing table.

Neighbor logs include information about the following events:

- The OSPFv3 neighbor state goes down.
- The OSPFv3 neighbor state goes backward because the local end receives BadLSReq, SeqNumberMismatch, and 1-Way events.

Examples

Display OSPFv3 LSA aging log information for OSPFv3 process 1.

```
<Sysname>display ospfv3 1 event-log lsa-flush

              OSPFv3 Process 1 with Router ID 1.3.3.3

 2014-09-02 07:55:25 Received MaxAge LSA from 1.1.1.1
 Type: 3   LS ID: 0.0.0.2         AdvRtr: 1.1.1.1           Seq#: 80000001

 2014-09-02 07:55:22 Flushed MaxAge LSA by itself
 Type: 3   LS ID: 0.0.0.2         AdvRtr: 1.3.3.3           Seq#: 80000001

 2014-09-02 07:55:07 Flushed MaxAge LSA by itself
 Type: 3   LS ID: 0.0.0.40        AdvRtr: 1.3.3.3           Seq#: 80000001

 2014-09-02 07:55:07 Flushed MaxAge LSA by itself
 Type: 3   LS ID: 0.0.0.39        AdvRtr: 1.3.3.3           Seq#: 80000001
```

Table 7 Command output

Field	Description
Received MaxAge LSA from X.X.X.X	The device received an LSA that has reached the maximum age from X.X.X.X.
Flushed MaxAge LSA by itself	The device flushed the LSA that has reached the maximum age.
Type	LSA type.
LS ID	LSA link state ID.
AdvRtr	Advertising router.
Seq#	LSA sequence number.

Display OSPFv3 route calculation log information for OSPFv3 process 1.

```
<Sysname>display ospfv3 1 event-log spf

              OSPFv3 Process 1 with Router ID 1.3.3.3

 Date       Time     Duration   Intra   Inter   External Reason
 2014-09-02 07:55:30 0.258827   0       0       0        Intra-area LSA
 2014-09-02 07:55:30 0.679      0       0       0        Intra-area LSA
 2014-09-02 07:55:30 0.51576    0       0       0        Intra-area LSA
 2014-09-02 07:55:30 0.372      0       0       0        Intra-area LSA
 2014-09-02 07:55:25 4.948353   0       0       0        Intra-area LSA
 2014-09-02 07:55:25 0.5288     0       0       0        Area 0 full neighbor
 2014-09-02 07:55:21 1.66013    0       0       0        Intra-area LSA
 2014-09-02 07:55:20 0.450905   0       0       0        Intra-area LSA
```

```
2014-09-02 07:55:15 0.253688   0       0       0       Interface state change
2014-09-02 07:55:15 0.5693     0       0       0       Intra-area LSA
```

Table 8 Command output

Field	Description
Date	Date when the route calculation starts, in YYYY-MM-DD format. YYYY represents the year, MM represents the month, and DD represents the day.
Time	Time when the route calculation starts, in hh:mm:ss format. hh represents the hour, mm represents the minutes, and ss represents the seconds.
Duration	Duration of the route calculation, in seconds.
Intra	Number of intra-area routes newly installed in the IPv6 routing table.
Inter	Number of inter-area routes newly installed in the IPv6 routing table.
External	Number of external routes newly installed in the IPv6 routing table.
Reason	Reasons why the route calculation is performed: • **Intra-area LSA**—Intra-area LSA changes. • **Inter-area LSA**—Inter-area LSA changes. • **External LSA**—External LSA changes. • **Configuration**—Configuration changes. • **Area 0 full neighbor**—Number of **FULL**-state neighbors in Area 0 changes. • **Area 0 up interface**—Number of interfaces in up state in Area 0 changes. • **AS number**—AS number changes. • **ABR summarization**—ABR summarization changes. • **GR end**—GR ends. • **Routing policy**—Routing policy changes. • **Others**—Other reasons.

Display OSPFv3 neighbor log information for OSPFv3 process 1.

```
<Sysname> display ospfv3 1 event-log peer

              OSPFv3 Process 1 with Router ID 1.1.1.1

Date       Time     Router ID       Reason       InstID  Interface
2014-09-02 16:39:13 1.3.3.3         IntPhyChange 0       Vlan101
2014-09-02 16:36:46 1.3.3.3         IntPhyChange 0       Vlan101
2014-09-02 16:34:49 1.3.3.3         BFDDown      0       Vlan101
2014-09-02 10:08:45 1.3.3.3         DeadExpired  0       Vlan102
2014-09-02 10:08:39 1.3.3.3         DeadExpired  0       VLINK1
2014-09-02 10:08:08 1.3.3.3         BFDDown      0       Vlan101
```

Table 9 Command output

Field	Description
Date	Date when the neighbor state changes, in YYYY-MM-DD format. YYYY represents the year, MM represents the month, and DD represents the day.

Field	Description
Time	Time when the neighbor state changes, in hh:mm:ss format. hh represents the hour, mm represents the minutes, and ss represents the seconds.
Router ID	Neighbor router ID.
Reason	Reasons for neighbor state changes: • **ResetConnect**—The connection is lost due to insufficient memory. • **IntChange**—The interface parameter has changed. • **ResetOspfv3**—The OSPFv3 process is reset. • **UndoOspfv3**—The OSPFv3 process is deleted. • **UndoArea**—The OSPFv3 area is deleted. • **UndoInt**—The interface is disabled. • **IntLogChange**—The logical attribute of the interface has changed. • **IntPhyChange**—The physical attribute of the interface has changed. • **DeadExpired**—The dead timer expires. • **Retrans**—Excessive retransmissions. • **BFDDown**—The interface is shut down by BFD. • **SilentInt**—The interface is configured as a silent interface. • **ConfStubArea**—The interface is configured with stub area parameters. • **ConfNssaArea**—The interface is configured with NSSA area parameters. • **VlinkDown**—The virtual link goes down. • **BadLSReq**—The interface receives BadLSReq events. • **SeqMismatch**—The interface receives SeqNumberMismatch events. • **Way**—The interface receives 1-Way events.
InstID	Instance ID for an interface.
Interface	Interface name.

display ospfv3 graceful-restart

Use **`display ospfv3 graceful-restart`** to display GR information.

Syntax

`display ospfv3` [*`process-id`*] **`graceful-restart`** [**`verbose`**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

`process-id`: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays GR information for all processes.

verbose: Displays detailed GR information. If you do not specify this keyword, the command displays brief GR information.

Examples

Display brief GR information for all OSPFv3 processes (GR restarter).

```
<Sysname> display ospfv3 graceful-restart

              OSPFv3 Process 1 with Router ID 3.3.3.3

 Graceful-restart capability     : Enable
 Graceful-restart support        : Planned and unplanned, Partial
 Helper capability               : Enable
 Helper support                  : Planned and unplanned
 Current GR state                : Normal
 Graceful-restart period         : 120 seconds
 Number of neighbors under helper: 0
 Number of restarting neighbors  : 0
 Last exit reason:
   Restarter: None
   Helper   : None
```

Table 10 Command output

Field	Description
OSPFv3 Process 1 with Router ID 3.3.3.3	The GR status of OSPFv3 process 1 with router ID 3.3.3.3 is displayed.
Graceful-restart capability	Whether OSPFv3 GR is enabled: • Enabled. • Disabled.
Graceful-restart support	GR modes that the process supports (displayed only when GR is enabled): • **Planned and unplanned**—Supports both planned and unplanned GR. • **Planned only**—Supports only planned GR. • **Partial**—Supports partial GR. • **Global**—Supports global GR.
Helper capability	Whether OSPFv3 GR helper is enabled: • Enabled. • Disabled.
Helper support	Policies and GR modes that the GR helper supports (displayed only when GR helper is enabled): • **Strict LSA check**—The GR helper supports strict LSA checking. • **Planned and unplanned**—The GR helper supports both planned and unplanned GR. • **Planned only**—The GR helper supports only planned GR.

Field	Description
Current GR state	GR status: • **Normal**—GR is not in progress or has completed. • **Under GR**—GR is in progress. • **Under Helper**—The process is acting as GR helper.
Graceful-restart period	GR restart interval.
Number of neighbors under helper	Number of neighbors in GR helper status.
Number of restarting neighbors	Number of neighbors in GR restarter status.

Last exit reason	Last exit reason:
	• **Restarter**—Reason that the restarter exited most recently:
	  ○ None.
	  ○ **Completed**—GR is completed.
	  ○ **Interval timer is fired**—The GR timer expires.
	  ○ **Interface state change**—An interface state change occurs.
	  ○ **Received 1-way hello**—The device receives 1-way hello packets from the neighbor.
	  ○ **Reset neighbor**—The neighbor is reset.
	  ○ **DR or BDR change**—The DR or BDR changes.
	• **Helper**—Reason that the helper exited most recently:
	  ○ None.
	  ○ **Completed**—GR is completed.
	  ○ **Received 1-way hello**—The device receives 1-way hello packets from the neighbor.
	  ○ **Grace Period timer is fired**—The GR timer expires.
	  ○ **Lsa check failed**—An LSA change on the GR helper is detected.
	  ○ **Reset neighbor**—The neighbor is reset.
	  ○ **Received MAXAGE gracelsa but neighbor is not full**—The device receives Grace-LSAs that reached the maximum age, but the neighbor is not in Full state.

Display detailed GR information for all OSPFv3 processes (GR restarter).

```
<Sysname> display ospfv3 graceful-restart verbose

               OSPFv3 Process 1 with Router ID 3.3.3.3

 Graceful-restart capability     : Enable
 Graceful-restart support        : Planned and unplanned, Partial
 Helper capability               : Enable
 Helper support                  : Planned and unplanned
 Current GR state                : Normal
 Graceful-restart period         : 120 seconds
 Number of neighbors under helper: 0
 Number of restarting neighbors  : 0
 Last exit reason:
```

```
  Restarter: None
  Helper   : None

Area: 0.0.0.0
Area flag: Normal
Area up interface count: 1

Virtual-link Neighbor-ID: 100.1.1.1, Neighbor-state: Full
Restarter state: Normal   State: P-2-P    Type: Virtual
Interface: 6696 (Vlan-interface200), Instance-ID: 0
Local  IPv6 address: 200:1:FFFF::1
Remote IPv6 address: 201:FFFF::2
Transit area: 0.0.0.1
Last exit reason:
  Restarter: None
  Helper   : None
Neighbor       GR state       Last helper exit reason
100.1.1.1      Normal         None

Area: 0.0.0.1
Area flag: Transit
Area up interface count: 3

Interface: 5506 (Vlan-interface3), Instance-ID: 0
Restarter state: Normal   State: DR       Type: Broadcast
Last exit reason:
  Restarter: None
  Helper   : None
Neighbor count of this interface: 0
Number of neighbors under helper: 0

Interface: 6696 (Vlan-interface200), Instance-ID: 0
Restarter state: Normal   State: DR       Type: Broadcast
Last exit reason:
  Restarter: None
  Helper   : None
Neighbor count of this interface: 1
Number of neighbors under helper: 0
Neighbor       GR state       Last helper exit reason
100.1.1.1      Normal         None

Area: 0.0.0.5
Area flag: NSSANoSummaryNoImportRoute
7/5 translator state: Disabled
7/5 translate stability timer interval: 0
Area up interface count: 0
```

Table 11 Command output

Field	Description
Area	Area ID.
Area flag	Type of the area: • Normal. • Transit. • Stub. • **StubNoSummary**—Totally stub area. • NSSA. • **NSSANoSummary**—Totally NSSA area. • **NSSANoSummaryNoImportRoute**—Totally NSSA area with the **no-import-route** keyword configured.
7/5 translator state	State of the translator that translates Type-7 LSAs to Type-5 LSAs: • **Enabled**—The translator is specified through commands. • **Elected**—The translator is designated through election. • **Disabled**—The device is not a translator.
7/5 translate stability timer interval	Stability interval (in seconds) for Type-7 LSA-to-Type-5 LSA translation.
Area up interface count	Number of up interfaces in the area.
Interface	Interface in the area, or the output interface of the virtual link.
Restarter state	Restarter state on the interface.
State	Interface state.
Type	Interface network type.
Neighbor count of this interface	Number of neighbors on the interface.
Neighbor	Neighbor router ID.
GR state	Neighbor GR state: • **Normal**—GR is not in progress or has completed. • **Under GR**—GR is in process. • **Under Helper**—The process is acting as GR helper.
Last helper exit reason	Reason that the helper exited most recently.
Virtual-link Neighbor-ID	Router ID of the virtual link's neighbor.
Neighbor-State	Neighbor or virtual link state: Down, Init, 2-Way, ExStart, Exchange, Loading, and Full.
Local IPv6 address	Local IPv6 address of the neighbor relationship.
Remote IPv6 address	Peer IPv6 address of the neighbor relationship.
Transit area	Transit area ID.

display ospfv3 interface

Use **display ospfv3 interface** to display OSPFv3 interface information.

Syntax

display ospfv3 [*process-id*] **interface** [*interface-type interface-number* | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535.

interface-type interface-number: Specifies an interface by its type and number.

verbose: Displays detailed information about all OSPFv3 interfaces.

Usage guidelines

If you do not specify a process, this command displays brief OSPFv3 interface information for all processes.

If you do not specify the *interface-type interface-number* argument or the **verbose** keyword, this command displays brief information about all OSPFv3 interfaces.

Examples

Display OSPFv3 information about VLAN-interface 1.

```
<Sysname> display ospfv3 interface vlan-interface 1

               OSPFv3 Process 1 with Router ID 1.1.1.1

 Area: 0.0.0.0
----------------------------------------------------------------------------
 Vlan-interface1 is up, line protocol is up
  Interface ID 65697        Instance ID 0
  IPv6 prefixes
    FE80::200:12FF:FE34:1  (Link-Local address)
    2001::1
  Cost: 1       State: BDR       Type: Broadcast    MTU: 1500
  Priority: 1
  Designated router: 2.2.2.2
  Backup designated router: 1.1.1.1
  Timers: Hello 10, Dead 40, Poll 40, Retransmit 5, Transmit delay 1
  FRR backup: Enabled
  Neighbor count is 1, Adjacent neighbor count is 1
  Primary path detection mode: BFD echo
  IPsec profile name: profile001
  Keychain authentication: Enabled (test), inherited
  Exchanging/Loading neighbors: 0
```

```
Wait timer: Off,  LsAck timer: Off
Prefix-suppression is enabled
```

Table 12 Command output

Field	Description
Area	Area ID that the interface belongs to.
Interface ID	Interface ID.
Instance ID	Instance ID.
IPv6 prefixes	IPv6 prefix.
Cost	Cost value of the interface.
State	Interface state: • **DOWN**—No protocol traffic can be sent or received on the interface. • **Waiting**—The interface starts sending and receiving Hello packets. The router is trying to determine the identity of the (Backup) designated router for the network. • **P-2-P**—The interface will send Hello packets at the hello interval, and try to establish an adjacency with the neighbor. • **DR**—The router is the designated router on the network. • **BDR**—The router is the backup designated router on the network. • **DROther**—The router is a DR Other router on the attached network.
Type	Network type of the interface: PTP (P2P), PTMP (P2MP), Broadcast, or NBMA.
MTU	MTU value of the interface.
Priority	DR priority of the interface.
Designated router	DR on this link.
Backup designated router	BDR on this link.
Timers	Time intervals in seconds configured on the interface: • **Hello**—Hello interval. • **Dead**—Dead interval. • **Poll**—Polling interval on an NBMA network. • **Retransmit**—LSA retransmission interval.
Transmit Delay	LSA transmission delay on the interface, in seconds.
FRR backup	Whether LFA calculation is enabled on an interface: • **Enabled**. • **Disabled**.
Neighbor count	Number of neighbors on the interface.
Primary path detection mode	Primary link detection mode: • **BFD ctrl**—BFD control packet mode. • **BFD echo**—BFD echo packet mode.
Adjacent neighbor count	Number of adjacencies on the interface.
IPsec profile name	IPsec profile applied to the interface.

Field	Description
Keychain authentication: Enabled (test), inherited	Keychain authentication is enabled for the interface, and the keychain **test** is used. The **inherited** attribute indicates that the interface is using the authentication mode specified for the area to which the interface belongs.

display ospfv3 lsdb

Use **display ospfv3 lsdb** to display OSPFv3 LSDB information.

Syntax

display ospfv3 [*process-id*] **lsdb** [{ **external** | **grace** | **inter-prefix** | **inter-router** | **intra-prefix** | **link** | **network** | **nssa** | **router** | **unknown** [*type*] } [*link-state-id*] [**originate-router** *router-id* | **self-originate**] | **statistics** | **total** | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays LSDB information for all processes.

external: Displays AS external LSAs (Type-5 LSAs).

grace: Displays Grace-LSAs (Type-11 LSAs).

inter-prefix: Displays Inter-area-prefix LSAs (Type-3 LSAs).

inter-router: Displays Inter-area-router LSAs (Type-4 LSAs).

intra-prefix: Displays Intra-area-prefix LSAs (Type-9 LSAs).

link: Displays Link-LSAs (Type-8 LSAs).

network: Displays Network-LSAs (Type-2 LSAs).

nssa: Displays NSSA LSAs (Type-7 LSAs).

router: Displays Router-LSAs (Type-1 LSAs).

unknown: Displays unknown LSAs.

type: Specifies an LSA type, a hexadecimal string of 0 to ffff. If you do not specify this argument, the command displays all unknown LSAs.

link-state-id: Specifies a link state ID in IPv4 address format.

originate-router *router-id*: Specifies an advertising router by its ID.

self-originate: Displays locally originated LSAs.

statistics: Displays LSA statistics.

total: Displays the total number of LSAs in the LSDB.

verbose: Displays detailed information. If you do not specify this keyword, the command displays brief information.

Examples

Display OSPFv3 LSDB information.

```
<Sysname> display ospfv3 lsdb

               OSPFv3 Process 1 with Router ID 1.1.1.1

                  Link-LSA (Interface Vlan-interface100)
------------------------------------------------------------------------
 Link state ID   Origin router    Age   SeqNumber  Checksum  Prefix
 0.15.0.8        2.2.2.2          0691  0x80000041 0x8315         1
 0.0.0.3         1.1.1.1          0623  0x80000001 0x0fee         1

                  Router-LSA (Area 0.0.0.1)
------------------------------------------------------------------------
 Link state ID   Origin router    Age   SeqNumber  Checksum    Link
 0.0.0.0         1.1.1.1          0013  0x80000068 0x5d5f         2
 0.0.0.0         2.2.2.2          0024  0x800000ea 0x1e22         0

                  Network-LSA (Area 0.0.0.1)
------------------------------------------------------------------------
 Link state ID   Origin router    Age   SeqNumber  Checksum
 0.15.0.8        2.2.2.2          0019  0x80000007 0x599e

                  Intra-Area-Prefix-LSA (Area 0.0.0.1)
------------------------------------------------------------------------
 Link state ID   Origin router    Age   SeqNumber  Checksum  Prefix  Reference
 0.0.0.2         2.2.2.2          3600  0x80000002 0x2eed         2  Network-LSA
 0.0.0.1         2.2.2.2          0018  0x80000001 0x1478         1  Network-LSA
```

Table 13 Command output

Field	Description
Origin router	Originating router.
Age	Age of LSAs.
SeqNumber	LSA sequence number.
Checksum	LSA checksum.
Prefix	Number of prefixes.
Link	Number of links.
Reference	Type of referenced LSA.

Display Link LSA information in the LSDB.

```
<Sysname> display ospfv3 lsdb link

               OSPFv3 Process 1 with Router ID 1.1.1.1
                  Link-LSA (Interface Vlan-interface100)
------------------------------------------------------------------------
  LS age            : 833
```

```
  LS type           : Link-LSA
  Link state ID     : 0.15.0.8
  Originating router: 2.2.2.2
  LS seq number     : 0x80000041
  Checksum          : 0x8315
  Length            : 56
  Priority          : 1
  Options           : 0x000013 (-|R|-|x|E|V6)
  Link-Local address: fe80::200:5eff:fe00:100
  Number of prefixes: 1
      Prefix        : 1001::/64
      Prefix options: 0 (-|-|x|-|-)
```

Table 14 Command output

Field	Description
LS age	Age of LSA.
LS type	Type of LSA.
Link state ID	Link state ID.
Originating router	Originating router.
LS seq number	LSA sequence number.
Checksum	LSA checksum.
Length	LSA length.
Priority	Router priority.
Options	Options.
Link-Local address	Link-local address.
Number of prefixes	Number of prefixes.
Prefix	Address prefix.
Prefix options	Prefix options.

Display LSA statistics.

```
<System> display ospfv3 lsdb statistics

               OSPFv3 Process 1 with Router ID 1.1.1.1
------------------------------------------------------------------------------
 Area ID         Router Network IntePre  InteRou IntraPre NSSA
 0.0.0.1         2      0       0        0       2        0
 0.0.0.3         1      0       0        0       1        1
 Total           3      0       0        0       3        1
------------------------------------------------------------------------------
                 Link   Grace   ASE
 Total           4      0       0
```

Table 15 Command output

Field	Description
Area ID	Area ID.
Router	Number of Type-1 LSAs.
Network	Number of Type-2 LSAs.
IntePre	Number of Type-3 LSAs.
InteRou	Number of Type-4 LSAs.
IntraPre	Number of Type-9 LSAs.
NSSA	Number of Type-7 LSAs.
Link	Number of Type-8 LSAs.
Grace	Number of Type-11 LSAs.
ASE	Number of Type-5 LSAs.

Display detailed OSPFv3 LSDB information.

```
<Sysname> display ospfv3 lsdb verbose

               OSPFv3 Process 1 with Router ID 1.1.1.1

                  Link-LSA (Interface Vlan-interface100)
------------------------------------------------------------------------------
 Link state ID   Origin router    Age   SeqNumber  Checksum  Prefix
 0.15.0.8        2.2.2.2          0691  0x80000041 0x8315         1
                 SendCnt: 0       RxmtCnt: 0       Status: Stale
 0.0.0.3         1.1.1.1          0623  0x80000001 0x0fee         1
                 SendCnt: 0       RxmtCnt: 0       Status: Stale

                  Router-LSA (Area 0.0.0.1)
------------------------------------------------------------------------------
 Link state ID   Origin router    Age   SeqNumber  Checksum    Link
 0.0.0.0         1.1.1.1          0013  0x80000068 0x5d5f         2
                 SendCnt: 0       RxmtCnt: 0       Status: Stale
 0.0.0.0         2.2.2.2          0024  0x800000ea 0x1e22         0
                 SendCnt: 0       RxmtCnt: 0       Status: Stale

                  Network-LSA (Area 0.0.0.1)
------------------------------------------------------------------------------
 Link state ID   Origin router    Age   SeqNumber  Checksum
 0.15.0.8        2.2.2.2          0019  0x80000007 0x599e
                 SendCnt: 0       RxmtCnt: 0       Status: Stale

                  Intra-Area-Prefix-LSA (Area 0.0.0.1)
------------------------------------------------------------------------------
 Link state ID   Origin router    Age   SeqNumber  Checksum  Prefix  Reference
 0.0.0.2         2.2.2.2          3600  0x80000002 0x2eed         2  Network-LSA
                 SendCnt: 0       RxmtCnt: 0       Status: Stale
```

```
0.0.0.1         2.2.2.2          0018  0x80000001 0x1478         1  Network-LSA
                SendCnt: 0       RxmtCnt: 0       Status: Stale
```

Table 16 Command output

Field	Description
SendCnt	Number of interfaces to send the LSA.
RxmtCnt	Number of LSAs in the link state retransmission list.
Status	LSA status: • Normal. • Delayed. • **Maxage routed**—The LSA has reached its maximum age. • Self originated. • **Stale**—A self-originated LSA is received during the GR process.

display ospfv3 nexthop

Use **`display ospfv3 nexthop`** to display OSPFv3 next hop information.

Syntax

`display ospfv3` [*`process-id`*] **`nexthop`**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

`process-id`: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays next hop information for all OSPFv3 processes.

Examples

Display next hop information for OSPFv3 process 1.

```
<Sysname> display ospfv3 1 nexthop

              OSPFv3 Process 1 with Router ID 1.1.1.1

 Nexthop : FE80::20C:29FF:FED7:F308              Interface: Vlan102
 RefCount: 4                                     Status   : Valid
 NbrID   : 1.1.1.1                               NbrIntID : 21

 Nexthop : FE80::20C:29FF:FED7:F312              Interface: Vlan103
 RefCount: 3                                     Status   : Valid
 NbrID   : 1.1.1.1                               NbrIntID : 38
```

Table 17 Command output

Field	Description
Nexthop	Next hop address.
Interface	Output interface.
RefCount	Reference count (routes that use the next hop).
Status	Next hop status: valid or invalid.
NbrId	Neighbor router ID.
NbrIntID	Neighbor interface ID.

display ospfv3 non-stop-routing

Use **display ospfv3 non-stop-routing** to display OSPFv3 NSR information.

Syntax

display ospfv3 [*process-id*] **non-stop-routing**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays OSPFv3 NSR information for all OSPFv3 processes.

Examples

Display OSPFv3 NSR information.

```
<Sysname> display ospfv3 non-stop-routing

              OSPFv3 Process 1 with Router ID 3.3.3.3

 Nonstop Routing capability: Enabled
 Upgrade phase             : Normal
```

Table 18 Command output

Field	Description
Nonstop Routing capability	NSR status: enabled or disabled.
Upgrade phase	NSR phase: • **Normal**—Normal status. • **Preparation**—Upgrade preparation phase. • **Smooth**—Upgrade phase. • **Precalculation**—Route pre-calculation phase. • **Calculation**—Route calculation phase. • **Redistribution**—Route redistribution phase.

display ospfv3 peer

Use **display ospfv3 peer** to display information about OSPFv3 neighbors.

Syntax

display ospfv3 [*process-id*] [**area** *area-id*] **peer** [[*interface-type interface-number*] [**verbose**] | *peer-router-id* | **statistics**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify a process, this command displays neighbor information for all processes.

area *area-id*: Specifies an area by its ID, an IPv4 address or a decimal integer in the range of 0 to 4294967295 that is translated into the IPv4 address format. If you do not specify an area, this command displays neighbor information for all areas.

interface-type interface-number: Specifies an interface by its type and number.

verbose: Displays detailed neighbor information.

peer-router-id: Specifies a neighbor.

statistics: Displays OSPFv3 neighbor statistics.

Usage guidelines

If you do not specify an interface and a neighbor, this command displays neighbor information for all interfaces.

Examples

Display neighbor information for OSPFv3 process 1.

```
<Sysname> display ospfv3 1 peer vlan-interface 1

              OSPFv3 Process 1 with Router ID 1.1.1.1

 Area: 0.0.0.1
----------------------------------------------------------------------------
 Router ID       Pri State            Dead-Time InstID Interface
 2.2.2.2         1   Init/ -          00:00:36  0      Vlan1
```

Table 19 Command output

Field	Description
Router ID	Neighbor router ID.
Pri	Neighboring router priority.
State	Neighbor state.
Dead-Time	Dead time remained.
InstID	Instance ID.

Field	Description
Interface	Interface connected to the neighbor.

Display detailed neighbor information for OSPFv3 process 1.

```
<Sysname> display ospfv3 1 peer vlan-interface 1 verbose

              OSPFv3 Process 1 with Router ID 1.1.1.1

 Area 0.0.0.1 interface Vlan1's neighbors
 Router ID: 2.2.2.2          Address: FE80::200:5EFF:FE00:100
   State: ExStart  Mode: None  Priority: 1
   DR: 2.2.2.2  BDR: None   MTU: 1500
   Options is 0x000413 (AT|-|-|-|-|-|R|-|x|E|V6)
   Dead timer due in 00:00:33
   Neighbor is up for 00:24:19
   Authentication sequence: (high) 0, (low) 59755
   Neighbor state change count: 205
   Database Summary List 0
   Link State Request List 0
   Link State Retransmission List 0
   Neighbor interface ID: 8037
   GR state: Normal
   Grace period: 0           Grace period timer: Off
   DD Rxmt Timer: Off        LS Rxmt Timer: On
```

Table 20 Command output

Field	Description
Router ID	Neighbor router ID.
Address	Link-local address of the interface.
State	Neighbor state.
Mode	Neighbor mode for LSDB synchronization.
Priority	Neighboring router priority.
DR	DR on the interface's network segment.
BDR	BDR on the interface's network segment.
MTU	Interface MTU.

Field	Description
Options	LSA options: • **AT**—Whether the Authentication Trailer option is carried in packets. • **DC**—The originating router supports OSPFv3 over on-demand circuits. • **R**—Whether the originating router is an active router. • **N**—Whether the originating router supports NSSA LSAs. • **x**—Reserved. • **E**—Whether the originating router can receive AS External LSAs. • **V6**—Whether the originating router takes part in IPv6 route calculation.
Dead timer due in hh:mm:ss	Remaining time for the dead timer, in hh:mm:ss format. hh represents the hours, mm represents the minutes, and ss represents the seconds.
Neighbor is up for hh:mm:ss	Uptime for the neighbor, in hh:mm:ss format. hh represents the hours, mm represents the minutes, and ss represents the seconds.
Authentication sequence: (high) 0, (low) 59755	Authentication sequence number carried in the received packets. The high 32-bit value is 0, and the low 32-bit value is 59755.
Neighbor state change count	Count of neighbor state changes.
Database Summary List	Number of LSAs sent in DD packet.
Link State Request List	Number of LSAs in the link state request list.
Link State Retransmission List	Number of LSAs in the link state retransmission list.
Neighbor interface ID	Interface ID of the neighbor.
GR state	GR state: • **Normal**—GR is not in progress. • **Doing GR**—Acting as the GR restarter. • Complete GR. • **Helper**—Acting as the GR helper.
Grace period	Grace-LSA sending interval.
Grace period timer	Grace-LSA sending interval timer.
DD Rxmt Timer	DD packet retransmission timer.
LS Rxmt Timer	LSU retransmission timer.

Display OSPFv3 neighbor statistics.

```
<Sysname> display ospfv3 peer statistics

              OSPFv3 Process 1 with Router ID 1.1.1.1
----------------------------------------------------------------------------
 Area ID         Down Attempt Init 2-Way ExStart Exchange Loading Full Total
 0.0.0.0         0    0       0    0     0       0        0       1    1
 Total           0    0       0    0     0       0        0       1    1
```

Table 21 Command output

Field	Description
Area ID	Area ID.
Down	In this state, neighbor initial state, the router has not received any information from a neighboring router for a period of time.
Attempt	This state is available only in an NBMA network. In this state, the OSPFv3 router has not received any information from a neighbor for a period. The router can send Hello packets at a longer interval to keep the neighbor relationship.
Init	In this state, the device received a Hello packet from the neighbor but the packet contains no router ID of the neighbor. Mutual communication is not setup.
2-Way	Mutual communication between the router and its neighbor is available. DR/BDR election is finished under this state (or higher).
ExStart	In this state, the router decides on the initial DD sequence number and active/standby relationship of the two parties.
Exchange	In this state, the router exchanges DD packets with the neighbor.
Loading	In this state, the router sends LSRs to request the neighbor for needed LSAs.
Full	LSDB synchronization has been accomplished between neighbors.
Total	Total number of neighbors under the same state.

display ospfv3 request-queue

Use **display ospfv3 request-queue** to display OSPFv3 request list information.

Syntax

display ospfv3 [*process-id*] [**area** *area-id*] **request-queue** [*interface-type interface-number*] [*neighbor-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify an OSPFv3 process, this command displays OSPFv3 request list information for all OSPFv3 processes.

area *area-id*: Specifies an area by its ID, an IPv4 address or a decimal integer in the range of 0 to 4294967295 that is translated into the IPv4 address format. If you do not specify an OSPFv3 area, this command displays OSPFv3 request list information for all areas.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays OSPFv3 request list information for all interfaces.

neighbor-id: Specifies a neighbor's router ID. If you do not specify a neighbor, this command displays OSPFv3 request list information for all OSPFv3 neighbors.

Examples

Display OSPFv3 request list information.

```
<Sysname> display ospfv3 request-queue

               OSPFv3 Process 1 with Router ID 1.1.1.1

                   Area: 0.0.0.0
                   Interface Vlan-interface100
----------------------------------------------------------------------------
                   Nbr-ID 1.3.3.3 Request List
 Type    LinkState ID    AdvRouter       SeqNum       Age   CkSum
 0x4005  0.0.34.127      1.3.3.3         0x80000001   0027  0x274d
 0x4005  0.0.34.128      1.3.3.3         0x80000001   0027  0x2d45
 0x4005  0.0.34.129      1.3.3.3         0x80000001   0027  0x333d
 0x4005  0.0.34.130      1.3.3.3         0x80000001   0027  0x3935
```

Table 22 Command output

Field	Description
Area	Area ID.
Interface	Interface type and sequence number.
Nbr-ID	Neighbor ID.
Request list	Request list information.
Type	LSA type.
LinkState ID	Link state ID.
AdvRouter	Advertising router.
SeqNum	LSA sequence number.
Age	LSA age.
CkSum	Checksum.

display ospfv3 retrans-queue

Use **display ospfv3 retrans-queue** to display retransmission list information.

Syntax

display ospfv3 [*process-id*] [**area** *area-id*] **retrans-queue** [*interface-type interface-number*] [*neighbor-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify an OSPFv3 process, this command displays retransmission list information for all OSPFv3 processes.

area *area-id*: Specifies an area by its ID, an IPv4 address or a decimal integer in the range of 0 to 4294967295 that is translated into the IPv4 address format. If you do not specify an OSPFv3 area, this command displays retransmission list information for all OSPFv3 areas.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays retransmission list information for all interfaces.

neighbor-id: Specifies a neighbor's router ID. If you do not specify a neighbor, this command displays retransmission list information for all neighbors.

Examples

Display OSPFv3 retransmission list information.

```
<Sysname> display ospfv3 retrans-queue

                OSPFv3 Process 1 with Router ID 1.1.1.1

                    Area: 0.0.0.0
                    Interface Vlan-interface100
----------------------------------------------------------------------------
                    Nbr-ID 1.2.2.2 Retransmit List
 Type     LinkState ID    AdvRouter       SeqNum       Age   CkSum
 0x2009   0.0.0.0         1.3.3.3         0x80000001   3600  0x49fb
```

Table 23 Command output

Field	Description
Area	Area ID.
Interface	Interface type and sequence number.
Nbr-ID	Neighbor ID.
Retransmit List	Retransmission list information.
Type	LSA type.
LinkState ID	Link state ID.
AdvRouter	Advertising router.
SeqNum	LSA sequence number.
Age	LSA age.
CkSum	Checksum.

display ospfv3 routing

Use **display ospfv3 routing** to display OSPFv3 route information.

Syntax

display ospfv3 [*process-id*] **routing** [*ipv6-address prefix-length*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays the OSPFv3 route information for all processes.

ipv6-address prefix-length: Specifies an IPv6 address. The *ipv6-address* argument specifies an IPv6 prefix. The *prefix-length* argument specifies a prefix length in the range of 0 to 128.

Examples

Display OSPFv3 routing information.

```
<Sysname> display ospfv3 routing

              OSPFv3 Process 1 with Router ID 9.9.9.9
------------------------------------------------------------------------
 I  - Intra area route,  E1 - Type 1 external route,  N1 - Type 1 NSSA route
 IA - Inter area route,  E2 - Type 2 external route,  N2 - Type 2 NSSA route
 *  - Selected route

*Destination: 1::/64
  Type       : IA                        Area       : 0.0.0.1
  AdvRouter  : 2.2.2.2                   Preference : 10
  NibID      : 0x23000003                Cost       : 2
  Interface  : Vlan10                    BkInterface: N/A
  Nexthop    : FE80::6AC7:45FF:FE5C:206
  BkNexthop  : N/A

 *Destination: 23::/64
  Type       : I                         Area       : 0.0.0.1
  AdvRouter  : 3.3.3.3                   Preference : 10
  NibID      : 0x23000001                Cost       : 1
  Interface  : Vlan10                    BkInterface: N/A
  Nexthop    : ::
  BkNexthop  : N/A

 *Destination: 8::/64
  Type       : E2                        Tag        : 1
  AdvRouter  : 1.1.1.1                   Preference : 150
  NibID      : 0x23000004                Cost       : 1
  Interface  : Vlan10                    BkInterface: N/A
  Nexthop    : FE80::6AC7:45FF:FE5C:206
  BkNexthop  : N/A

 Total: 3
 Intra area: 3         Inter area: 0         ASE: 0         NSSA: 0
```

Table 24 Command output

Field	Description
Destination	Destination network segment.

Type	Route type.
Area	Area ID.
AdvRouter	Advertising router.
Preference	OSPFv3 route preference.
NibID	Next hop ID.
Cost	Route cost value.
Interface	Output interface.
BkInterface	Backup output interface.
Nexthop	Primary next hop IP address.
BkNexthop	Backup next hop IP address.
Interface	Output interface.
AdvRouter	Advertising router.
Area	Area ID.
Tag	Tag of external routes.
Preference	Route preference.
Total	Total number of routes.
Intra area	Number of intra-area routes.
Inter area	Number of inter-area routes.
ASE	Number of Type-5 external routes.
NSSA	Number of Type-7 external routes.

display ospfv3 spf-tree

Use **display ospfv3 spf-tree** to display OSPFv3 SPF tree information.

Syntax

display ospfv3 [*process-id*] [**area** *area-id*] **spf-tree** [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify a process, this command displays SPF tree information for all OSPFv3 processes.

area *area-id*: Specifies an OSPFv3 area by its ID. The area ID is an IP address or a decimal integer in the range of 0 to 4294967295 that is translated into the IP address format. If you do not specify an area, this command displays SPF tree information for all OSPFv3 areas.

verbose: Displays detailed OSPFv3 SPF tree information. If you do not specify this keyword, the command displays brief OSPFv3 SPF tree information.

Examples

Display brief SPF tree information for Area 0 in OSPFv3 process 1.

```
<Sysname> display ospfv3 1 area 0 spf-tree

               OSPFv3 Process 1 with Router ID 1.1.1.1

 Flags: S-Node is on SPF tree       R-Node is directly reachable
        I-Node or Link is init      D-Node or Link is to be deleted
        P-Neighbor is parent        A-Node is in candidate list
        C-Neighbor is child         H-Nexthop changed
        N-Link is a new path        V-Link is involved

                 Area: 0.0.0.0  Shortest Path Tree

 SPFNode         Type   Flag         SPFLink         Type   Cost  Flag
>1.1.1.1         Router S R
                                 -->2.2.2.2         RT2RT  1     C
                                 -->2.2.2.2         RT2RT  1     P
```

Table 25 Command output

Field	Description
SPFNode	SPF node, represented by the advertising router ID. Node type: • **Network**—Network node. • **Router**—Router node. Node flag: • **I**—The node is in initialization state. • **A**—The node is on the candidate list. • **S**—The node is on the SPF tree. • **R**—The node is directly connected to the root node. • **D**—The node is to be deleted.
SPFLink	SPF link, representing the advertising router ID. Link type: • **RT2RT**—Router to router. • **NET2RT**—Network to router. • **RT2NET**—Router to network. Link flag: • **I**—The link is in initialization state. • **P**—The peer is the parent node. • **C**—The peer is the child node. • **D**—The link is to be deleted. • **H**—The next hop is changed. • **V**—When the peer node is deleted or added, the peer node is not on the SPF tree or is deleted. • **N**—The link is newly added, and both end nodes are on the SPF tree. • **L**—The link is on the area change list.

Display detailed topology information for Area 0 in OSPFv3 process 1.

```
<Sysname> display ospfv3 1 area 0 spf-tree verbose

               OSPFv3 Process 1 with Router ID 1.1.1.1

 Flags: S-Node is on SPF tree       R-Node is directly reachable
        I-Node or Link is init      D-Node or Link is to be deleted
        P-Neighbor is parent        A-Node is in candidate list
        C-Neighbor is child         H-Nexthop changed
        N-Link is a new path        V-Link is involved

           Area: 0.0.0.0  Shortest Path Tree

>SPFNode[0]
  AdvID        : 1.1.1.1                 LsID       : 0.0.0.0
  NodeType     : Router                  Distance   : 1
  NodeFlag     : S R
  Nexthop count: 1
 -->NbrID      : 1.1.1.1                 NbrIntID   : 21
    Interface  : Vlan102                 NhFlag     : Valid
    BkInterface: Vlan103                RefCount    : 4
    Nexthop    : FE80::20C:29FF:FED7:F308
    BkNexthop  : FE80::4
  SPFLink count: 1
 -->AdvID      : 1.1.1.1                 LsID       : 0.0.0.0
    IntID      : 232                     NbrIntID   : 465
    NbrID      : 2.2.2.2                 LinkType   : RT2RT
    LinkCost   : 1                       LinkNewCost: 1
    LinkFlag   : C                       NexthopCnt : 0
  ParentLink count: 1
 -->AdvID      : 1.1.1.1                 LsID       : 0.0.0.0
    IntID      : 215                     NbrIntID   : 466
    NbrID      : 2.2.2.2                 LinkType   : RT2RT
    LinkCost   : 1                       LinkNewCost: 1
    LinkFlag   : P                       NexthopCnt : 0
```

Table 26 Command output

Field	Description
SPFNode	SPF node.
AdvID	ID of the advertising router.
LsID	Link state ID.
NodeType	Node type.
Distance	Cost to the root node.
NodeFlag	Node flag.
Nexthop count	Number of next hops.
NbrID	Neighbor router ID.
NbrIntID	Neighbor interface ID.

Field	Description
Interface	Output interface.
NhFlag	Next hop flag: valid or invalid.
BkInterface	Backup output interface.
RefCount	Reference count (routes that use the backup next hop).
Nexthop	Next hop.
BkNexthop	Backup next hop.
SPFLink count	Number of SPF links.
IntID	Interface ID.
LinkType	Link type: • **RT2RT**—Router to router. • **NET2RT**—Network to router. • **RT2NET**—Router to network.
LinkCost	Link cost.
LinkNewCost	New link cost.
LinkFlag	Link flag: • **I**—The link is in initialization state. • **P**—The peer is the parent node. • **C**—The peer is the child node. • **D**—The link is to be deleted. • **H**—The next hop is changed. • **V**—When the peer node is deleted or added, the peer node is not on the SPF tree or is deleted. • **N**—The link is newly added, and both end nodes are on the SPF tree. • **L**—The link is on the area change list.
NexthopCnt	Number of next hops.
ParentLinkCnt	Number of parent links.

display ospfv3 statistics

Use **display ospfv3 statistics** to display OSPFv3 statistics.

Syntax

display ospfv3 [*process-id*] **statistics** [**error** | **packet** [*interface-type interface-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays OSPFv3 statistics for all processes.

error: Displays error statistics. If you do not specify this keyword, the command displays OSPFv3 packet, LSA, and route statistics.

packet: Displays packet statistics.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify this argument, the command displays statistics for all interfaces.

Examples

Display OSPFv3 statistics.

```
<Sysname> display ospfv3 statistics

              OSPFv3 Process 1 with Router ID 1.1.1.1
                  Packet Statistics
------------------------------------------------------------
 Type                         Recv               Send
 Hello                        1746               1284
 DB Description               505                941
 Ls Req                       252                136
 Ls Upd                       851                1553
 Ls Ack                       416                450

            Local Originated LSAs Statistics
------------------------------------------------------------
 Type                                           Count
 Router-LSA                                     192
 Network-LSA                                    0
 Inter-Area-Prefix-LSA                          0
 Inter-Area-Router-LSA                          0
 AS-external-LSA                                0
 NSSA-LSA                                       0
 Link-LSA                                       10
 Intra-Area-Prefix-LSA                          112
 Grace-LSA                                      0
 Unknown-LSA                                    0
 Total                                          314

                  Routes Statistics
------------------------------------------------------------
 Type                                           Count
 Intra Area                                     0
 Inter Area                                     0
 ASE                                            0
 NSSA                                           0
```

Table 27 Command output

Field	Description
Packet Statistics	Statistics about inbound and outbound packets.
Hello	Hello packet.
DB Description	DB description packet.
Ls Req	Link state request packet.
Ls Upd	Link state update packet.
Ls Ack	Link state acknowledgment packet.
Local Originated LSAs Statistics	Statistics about generated LSAs.
Router-LSA	Number of Type-1 LSAs.
Network-LSA	Number of Type-2 LSAs.
Inter-Area-Prefix-LSA	Number of Type-3 LSAs.
Inter-Area-Router-LSA	Number of Type-4 LSAs.
AS-external-LSA	Number of Type-5 LSAs.
NSSA-LSA	Number of Type-7 LSAs.
Link-LSA	Number of Type-8 LSAs.
Intra-Area-Prefix-LSA	Number of Type-9 LSAs.
Grace-LSA	Number of Type-11 LSAs.
Unknown-LSA	Number of Unknown-LSAs.
Total	Total number.
Routes Statistics	Number of routes.
Intra Area	Intra-area routes.
Inter Area	Inter-area routes.
ASE	Type-5 external routes.
NSSA	Type-7 external routes.

Display OSPFv3 error statistics.

```
<Sysname> display ospfv3 statistics error

                OSPFv3 Process 1 with Router ID 1.1.1.1

 0          : Transmit error               0          : Neighbor state low
 0          : Packet too small             0          : Bad version
 0          : Bad checksum                 0          : Unknown neighbor
 0          : Bad area ID                  0          : Bad packet
 0          : Packet dest error            0          : Inactive area packet
 0          : Router ID confusion          0          : Bad virtual link
 0          : HELLO: Hello-time mismatch   0          : HELLO: Dead-time mismatch
 0          : HELLO: Ebit option mismatch  0          : DD: Ebit option mismatch
 0          : DD: Unknown LSA type         0          : DD: MTU option mismatch
 0          : REQ: Empty request           0          : REQ: Bad request
```

```
0          : UPD: LSA checksum bad        0          : UPD: Unknown LSA type
0          : UPD: Less recent LSA         0          : UPD: LSA length bad
0          : UPD: LSA AdvRtr id bad       0          : ACK: Bad ack packet
0          : ACK: Invalid ack             0          : Interface down
0          : Multicast incapable          0          : Authentication failure
0          : AuthSeqNumber error
```

Table 28 Command output

Field	Description
Transmit error	Packets with error when being transmitted.
Neighbor state low	Packets received in low neighbor state.
Packet too small	Packets too small in length.
Bad version	Packets with wrong version.
Bad checksum	Packets with wrong checksum.
Unknown neighbor	Packets received from unknown neighbors.
Bad area ID	Packets with invalid area ID.
Bad packet	Packets illegal.
Packet dest error	Packets with wrong destination addresses.
Inactive area packet	Packets received in inactive areas.
Router ID confusion	Packets with duplicate router ID.
Bad virtual link	Packets on wrong virtual links.
HELLO: Hello-time mismatch	Hello packets with mismatched hello timer.
HELLO: Dead-time mismatch	Hello packets with mismatched dead timer.
HELLO: Ebit option mismatch	Hello packets with mismatched E-bit in the option field.
DD: Ebit option mismatch	DD packets with mismatched E-bit in the option field.
DD: Unknown LSA type	DD packets with unknown LSA type.
DD: MTU option mismatch	DD packets with mismatched MTU.
REQ: Empty request	LSR packets with no request information.
REQ: Bad request	Bad LSR packets.
UPD: LSA checksum bad	LSU packets with wrong LSA checksum.
UPD: Unknown LSA type	LSU packets with unknown LSA type.
UPD: Less recent LSA	LSU packets without the most recent LSA.
UPD: LSA length bad	LSU packets with wrong LSA length.
UPD: LSA AdvRtr id bad	LSU packets with wrong LSA advertising router.
ACK: Bad ack packet	Bad LSAck packets for LSU packets.
ACK: Invalid ack	Invalid LSAck packets.
Interface down	Shutdown times of the interface.
Multicast incapable	Failures to join the multicast group.
Authentication failure	Failures to authenticate the received packets.

Field	Description
AuthSeqNumber error	Authentication sequence number errors in the received packets.

Display OSPFv3 packet statistics for all processes and interfaces.

```
<Sysname>display ospfv3 statistics packet

          OSPFv3 Process 1 with Router ID 1.1.1.1

         Hello      DD         LSR        LSU        ACK        Total
 Input : 8727       128        28         1584       929        11396
 Output: 8757       159        86         987        1513       11502

 Area: 0.0.0.0

 Area: 0.0.0.1
 Interface: Vlan-interface101
         DD         LSR        LSU        ACK        Total
 Input : 16         0          45         7          68
 Output: 17         1          7          44         69
 Interface: Vlan-interface102
         DD         LSR        LSU        ACK        Total
 Input : 41         13         720        719        1493
 Output: 54         41         750        713        1558
```

Table 29 Command output

Field	Description
Total	Total number of packets.
Input	Number of received packets.
Output	Number of sent packets.
Area	Area ID.
Interface	Interface name.

display ospfv3 vlink

Use **display ospfv3 vlink** to display OSPFv3 virtual link information.

Syntax

display ospfv3 [*process-id*] **vlink**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command displays the OSPFv3 virtual link information for all OSPFv3 processes.

Examples

Display OSPFv3 virtual link information.

```
<Sysname> display ospfv3 vlink

              OSPFv3 Process 1 with Router ID 1.1.1.1

 Virtual-link Neighbor-ID: 12.2.2.2, Neighbor-state: Full
 Interface: 2348 (Vlan-interface12), Instance-ID: 0
 Local  IPv6 address: 3:3333::12
 Remote IPv6 address: 2:2222::12
 Cost: 1  State: P-2-P  Type: Virtual
 Transit area: 0.0.0.1
 Timers: Hello 10, Dead 40, Retransmit 5, Transmit delay 1
 IPsec profile name: profile001
 Keychain authentication: Enabled (test), inherited
```

Table 30 Command output

Field	Description
Virtual-link Neighbor-ID	ID of the neighbor on the virtual link.
Neighbor-State	Neighbor state: Down, Init, 2-Way, ExStart, Exchange, Loading, or Full.
Interface	Number and name of the local interface on the virtual link.
Cost	Interface route cost.
State	Interface state.
Type	Virtual link.
Transit Area	Transit area ID. This field is displayed when a virtual link is present on the interface.
Timers	Values of OSPFv3 timers (in seconds): **Hello**, **Dead**, and **Retransmit**.
Transmit delay	LSA transmission delay on the interface, in seconds.
IPsec profile name	IPsec profile applied to the virtual link.
Keychain authentication: Enabled (test), inherited	Keychain authentication is enabled for the virtual link, and the keychain **test** is used. The **inherited** attribute indicates that the virtual link is using the authentication mode specified for the backbone area.

enable ipsec-profile

Use **enable ipsec-profile** to apply an IPsec profile to an OSPFv3 area.

Use **undo enable ipsec-profile** to remove the IPsec profile from the OSPFv3 area.

Syntax

enable ipsec-profile *profile-name*

undo enable ipsec-profile

Default

No IPsec profile is applied to an area.

Views

OSPFv3 area view

Predefined user roles

network-admin

Parameters

profile-name: Specifies an IPsec profile by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

To protect routing information and prevent attacks, OSPFv3 can authenticate protocol packets by using an IPsec profile. For more information about IPsec profiles, see *Security Configuration Guide*.

Examples

Apply IPsec profile **profile001** to Area 0 in OSPFv3 process 1.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 0
[Sysname-ospfv3-1-area-0.0.0.0] enable ipsec-profile profile001
```

event-log

Use **event-log** to set the maximum number of OSPFv3 logs.

Use **undo event-log** to remove the configuration.

Syntax

event-log { **lsa-flush** | **peer** | **spf** } **size** *count*

undo event-log { **lsa-flush** | **peer** | **spf** } **size**

Default

The maximum number of LSA aging logs, neighbor logs, or route calculation logs is 10.

Views

OSPFv3 view

Predefined user roles

network-admin

Parameters

lsa-flush: Specifies the maximum number of LSA aging logs.

peer: Specifies the maximum number of neighbor logs.

spf: Specifies the maximum number of route calculation logs.

size *count*: Specifies the maximum number of OSPFv3 logs, in the range of 0 to 65535.

Examples

Set the maximum number of route calculation logs to 50 in OSPFv3 process 100.

```
<Sysname> system-view
[Sysname] ospfv3 100
```

```
[Sysname-ospfv3-100] event-log spf size 50
```

fast-reroute (OSPFv3 view)

Use **fast-reroute** to configure OSPFv3 FRR.

Use **undo fast-reroute** to restore the default.

Syntax

fast-reroute { **lfa** [**abr-only**] | **route-policy** *route-policy-name* }

undo fast-reroute

Default

OSPFv3 FRR is disabled.

Views

OSPFv3 view

Predefined user roles

network-admin

Parameters

lfa: Uses the LFA algorithm to calculate a backup next hop for all routes.

abr-only: Uses the next hop of the route to the ABR as the backup next hop.

route-policy *route-policy-name*: Uses a routing policy to designate a backup next hop. The *route-policy-name* argument is a case-sensitive string of 1 to 63 characters.

Usage guidelines

Do not use the **fast-reroute lfa** command together with the **vlink-peer** command.

Examples

Enable FRR to calculate a backup next hop for all routes by using LFA algorithm in OSPFv3 process 1.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] fast-reroute lfa
```

filter (OSPFv3 area view)

Use **filter** to configure inbound/outbound Inter-Area-Prefix-LSA filtering on an ABR.

Use **undo filter** to remove the configuration.

Syntax

filter { *ipv6-acl-number* | **prefix-list** *prefix-list-name* | **route-policy** *route-policy-name* } { **export** | **import** }

undo filter { **export** | **import** }

Default

Inter-Area-Prefix-LSAs are not filtered.

Views

OSPFv3 area view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies an IPv6 ACL by its number in the range of 2000 to 3999 to filter inbound/outbound Inter-Area-Prefix-LSAs.

prefix-list *prefix-list-name*: Specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter inbound/outbound Inter-Area-Prefix-LSAs.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to filter inbound/outbound Inter-Area-Prefix-LSAs.

export: Filters Inter-Area-Prefix-LSAs advertised to other areas.

import: Filters Inter-Area-Prefix-LSAs advertised into the local area.

Usage guidelines

This command applies only to an ABR.

Examples

Use IPv6 prefix list **my-prefix-list** to filter inbound Inter-Area-Prefix-LSAs. Use IPv6 basic ACL 2000 to filter outbound Inter-Area-Prefix-LSAs in OSPFv3 Area 1.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 1
[Sysname-ospfv3-1-area-0.0.0.1] filter prefix-list my-prefix-list import
[Sysname-ospfv3-1-area-0.0.0.1] filter 2000 export
```

filter-policy export (OSPFv3 view)

Use **filter-policy export** to configure OSPFv3 to filter redistributed routes.

Use **undo filter-policy export** to remove the configuration.

Syntax

filter-policy { *ipv6-acl-number* | **prefix-list** *prefix-list-name* } **export** [**direct** | { **ospfv3** | **ripng** } [*process-id*] | **static**]

undo filter-policy export [**direct** | { **ospfv3** | **ripng** } [*process-id*] | **static**]

Default

Redistributed routes are not filtered.

Views

OSPFv3 view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies an IPv6 ACL by its number in the range of 2000 to 3999 to filter redistributed routes by destination address.

prefix-list *prefix-list-name*: Specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter redistributed routes by destination address.

direct: Filters redistributed direct routes.

ospfv3: Filters redistributed OSPFv3 routes.

ripng: Filters redistributed RIPng routes.

process-id: Specifies a process by its ID in the range of 1 to 65535. The default value is 1.

static: Filters redistributed static routes.

Usage guidelines

To use an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL in one of the following ways:

- To deny/permit a route with the specified destination, use **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix*.
- To deny/permit a route with the specified destination and prefix, use **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix* **destination** *dest dest-prefix*.

The **source** keyword specifies the destination address of a route, and the **destination** keyword specifies the prefix of the route. For the configuration to take effect, specify a contiguous prefix.

Using the **filter-policy export** command filters only routes redistributed by the **import-route** command. If the **import-route** command is not configured to redistribute routes from other protocols and other OSPFv3 processes, the **filter-policy export** command does not take effect.

If you do not specify a routing protocol, the command filters all redistributed routes.

Examples

Use IPv6 prefix list **abc** to filter redistributed routes.

```
<Sysname> system-view
[Sysname] ipv6 prefix-list abc permit 2002:1:: 64
[Sysname] ospfv3
[Sysname-ospfv3-1] filter-policy prefix-list abc export
```

Configure IPv6 advanced ACL 3000 to permit only route 2001::1/128. Use ACL 3000 to filter redistributed routes.

```
<Sysname> system-view
[Sysname] acl ipv6 advanced 3000
[Sysname-acl-ipv6-adv-3000] rule 10 permit ipv6 source 2001::1 128 destination
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff 128
[Sysname-acl-ipv6-adv-3000] rule 100 deny ipv6
[Sysname-acl-ipv6-adv-3000] quit
[Sysname] ospfv3
[Sysname-ospfv3-1] filter-policy 3000 export
```

filter-policy import (OSPFv3 view)

Use **filter-policy import** to configure OSPFv3 to filter routes calculated using received LSAs.

Use **undo filter-policy import** to remove the configuration.

Syntax

filter-policy { *ipv6-acl-number* [**gateway** *prefix-list-name*] | **prefix-list** *prefix-list-name* [**gateway** *prefix-list-name*] | **gateway** *prefix-list-name* | **route-policy** *route-policy-name* } **import**

undo filter-policy import

Default

Routes calculated using received LSAs are not filtered.

Views

OSPFv3 view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies an IPv6 ACL by its number in the range of 2000 to 3999 to filter routes by destination.

gateway *prefix-list-name*: Specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter routes by next hop. If you do not specify this option, the command does not filter routes by next hop.

prefix-list *prefix-list-name*: Specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters, to filter routes by destination.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to filter received routes.

Usage guidelines

To use an advanced ACL (with a number from 3000 to 3999) in the command, configure the ACL in one of the following ways:

- To deny/permit a route with the specified destination, use **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix*.
- To deny/permit a route with the specified destination and prefix, use **rule** [*rule-id*] { **deny** | **permit** } **ipv6 source** *sour sour-prefix* **destination** *dest dest-prefix*.

The **source** keyword specifies the destination address of a route, and the **destination** keyword specifies the prefix of the route. For the configuration to take effect, specify a contiguous prefix.

Using the **filter-policy import** command filters only routes computed by OSPFv3. Routes that fail to pass the filter are not added to the routing table.

Examples

Use IPv6 prefix list **abc** to filter received routes.

```
<Sysname> system-view
[Sysname] ipv6 prefix-list abc permit 2002:1:: 64
[Sysname] ospfv3
[Sysname-ospfv3-1] filter-policy prefix-list abc import
```

Configure IPv6 advanced ACL 3000 to permit only route 2001::1/128 to pass. Use ACL 3000 to filter received routes.

```
<Sysname> system-view
[Sysname] acl ipv6 advanced 3000
[Sysname-acl-ipv6-adv-3000] rule 10 permit ipv6 source 2001::1 128 destination
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff 128
```

```
[Sysname-acl-ipv6-adv-3000] rule 100 deny ipv6
[Sysname-acl-ipv6-adv-3000] quit
[Sysname] ospfv3
[Sysname-ospfv3-1] filter-policy 3000 import
```

graceful-restart enable

Use **graceful-restart enable** to enable the GR capability for OSPFv3.

Use **undo graceful-restart enable** to disable the GR capability for OSPFv3.

Syntax

graceful-restart enable [**global** | **planned-only**] *

undo graceful-restart enable

Default

The GR capability for OSPFv3 is disabled.

Views

OSPFv3 view

Predefined user roles

network-admin

Parameters

global: Enables global GR. In global GR mode, a GR process can be completed only when all GR helpers exist. A GR process fails if a GR helper fails (for example, the interface connected to the GR helper goes down). If you do not specify this keyword, the command enables partial GR. In partial GR mode, a GR process can be completed as long as one GR helper exists.

planned-only: Enables planned GR only. If you do not specify this keyword, the command enables both planned GR and unplanned GR.

Usage guidelines

GR includes planned GR and unplanned GR.

- **Planned GR**—Manually restarts OSPFv3 or performs an active/standby switchover. Before OSPFv3 restart or active/standby switchover, the GR restarter sends Grace-LSAs to GR helpers.
- **Unplanned GR**—OSPFv3 restarts or an active/standby switchover occurs because of device failure. Before OSPFv3 restart or active/standby switchover, the GR restarter does not send Grace-LSAs to GR helpers.

OSPFv3 GR and OSPFv3 NSR are mutually exclusive. Do not configure the **graceful-restart enable** command and the **non-stop-routing** command at the same time.

To prevent service interruption after a master/backup switchover, a GR restarter running OSPFv3 must perform the following tasks:

- Keep the GR restarter forwarding entries stable during reboot.
- Establish all adjacencies and obtain complete topology information after reboot.

Examples

Enable the GR capability for OSPFv3 process 1.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] graceful-restart enable
```

Related commands

graceful-restart helper enable

graceful-restart helper enable

Use **graceful-restart helper enable** to enable the GR helper capability for OSPFv3.

Use **undo graceful-restart helper enable** to disable the GR helper capability for OSPFv3.

Syntax

graceful-restart helper enable [**planned-only**]

undo graceful-restart helper enable

Default

The GR helper capability for OSPFv3 is enabled.

Views

OSPFv3 view

Predefined user roles

network-admin

Parameters

planned-only: Enables only planned GR for the GR helper. If you do not specify this keyword, the command enables both planned GR and unplanned GR for the GR helper.

Usage guidelines

Upon receiving the Grace-LSA, the neighbors with the GR helper capability enter the helper mode (and are called GR helpers). Then, the GR restarter retrieves its adjacencies and LSDB with the help of the GR helpers.

Examples

Enable the GR helper capability for OSPFv3 process 1.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] graceful-restart helper enable
```

Related commands

graceful-restart enable

graceful-restart helper strict-lsa-checking

Use **graceful-restart helper strict-lsa-checking** to enable strict LSA checking for the GR helper.

Use **undo graceful-restart helper strict-lsa-checking** to disable strict LSA checking for the GR helper.

Syntax

graceful-restart helper strict-lsa-checking

undo graceful-restart helper strict-lsa-checking

Default

Strict LSA checking for the GR helper is disabled.

Views

OSPFv3 view

Predefined user roles

network-admin

Usage guidelines

With GR helper enabled, when an LSA change on the GR helper is detected, the GR helper device exits the GR helper mode.

Examples

Enable strict LSA checking for the GR helper in OSPFv3 process 1.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] graceful-restart helper strict-lsa-checking
```

Related commands

graceful-restart helper enable

graceful-restart interval

Use **graceful-restart interval** to set the GR restart interval.

Use **undo graceful-restart interval** to restore the default.

Syntax

graceful-restart interval *interval*

undo graceful-restart interval

Default

The GR restart interval is 120 seconds.

Views

OSPFv3 view

Predefined user roles

network-admin

Parameters

interval: Specifies GR restart interval in the range of 40 to 1800 seconds.

Usage guidelines

For GR restart to succeed, the value of the GR restart interval cannot be smaller than the maximum OSPFv3 neighbor dead time of all the OSPFv3 interfaces.

Examples

Set the GR restart interval for OSPFv3 process 1 to 100 seconds.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] graceful-restart interval 100
```

Related commands

ospfv3 timer dead

import-route (OSPFv3 view)

Use **import-route** to redistribute routes.

Use **undo import-route** to disable route redistribution.

Syntax

import-route { **direct** | **static** } [**cost** *cost-value* | **nssa-only** | **route-policy** *route-policy-name* | **tag** *tag* | **type** *type*] *

import-route { **ospfv3** | **ripng** } [*process-id* | **all-processes**] [**allow-direct** | **cost** *cost-value* | **nssa-only** | **route-policy** *route-policy-name* | **tag** *tag* | **type** *type*] *

undo import-route { | **direct** | { **ospfv3** | **ripng** } [*process-id* | **all-processes**] | **static** }

Default

OSPFv3 route redistribution is disabled.

Views

OSPFv3 view

Predefined user roles

network-admin

Parameters

direct: Redistributes direct routes.

static: Redistributes static routes.

ospfv3: Redistributes OSPFv3 routes.

ripng: Redistributes RIPng routes.

process-id: Specifies the process ID of a routing protocol, in the range of 1 to 65536. The default is 1.

all-processes: Redistributes routes from all the processes of the specified routing protocol.

allow-direct: Redistributes the networks of the local interfaces enabled with the specified routing protocol. If you do not specify this keyword, the networks of the local interfaces are not redistributed. If you specify both the **allow-direct** keyword and the **route-policy** *route-policy-name* option, make sure the **if-match** rule defined in the routing policy does not conflict with the **allow-direct** keyword. For example, if you specify the **allow-direct** keyword, do not configure the **if-match route-type** rule for the routing policy. Otherwise, the **allow-direct** keyword does not take effect.

cost *cost-value*: Specifies a cost for redistributed routes, in the range of 1 to 16777214. If you do not specify a cost, the cost for redistributed routes is 1.

nssa-only: Limits the route advertisement to the NSSA area by setting the P-bit of Type-7 LSAs to 0. If you do not specify this keyword, the P-bit of Type-7 LSAs is set to 1. If the router acts as both an ASBR and an ABR and **FULL** state neighbors exist in the backbone area, the P-bit of Type-7 LSAs originated by the router is set to 0. This keyword applies to NSSA routers.

route-policy *route-policy-name*: Specifies a routing policy to filter redistributed routes. The *route-policy-name* argument is a case-sensitive string of 1 to 63 characters.

tag *tag*: Specifies a tag for external LSAs, in the range of 0 to 4294967295. If you do not specify this option, the tag specified by the **default tag** command applies.

type *type*: Specifies the type for redistributed routes, 1 or 2. The default is 2.

Usage guidelines

An external route is a route to a destination outside the OSPFv3 AS. External routes include the following types:

- **Type-1 external routes**—Have high credibility. The cost of Type-1 external routes is comparable with the cost of OSPFv3 internal routes. The cost of a Type-1 external route equals the cost from the router to the ASBR plus the cost from the ASBR to the external route's destination.
- **Type-2 external routes**—Have low credibility. OSPFv3 considers the cost from the ASBR to a Type-2 external route is much bigger than the cost from the ASBR to an OSPFv3 internal router. The cost of a Type-2 external route equals the cost from the ASBR to the Type-2 external route's destination.

The **import-route** command cannot redistribute default routes.

The **import-route nssa-only** command redistributes AS-external routes in Type-7 LSAs only into the NSSA area.

Examples

Configure OSPFv3 process 1 to redistribute routes from RIPng and specify the type as type 2 and cost as 50.

```
<Sysname> system-view
[Sysname] ospfv3
[Sysname-ospfv3-1] import-route ripng 10 type 2 cost 50
```

Configure OSPFv3 process 100 to redistribute the routes discovered by OSPFv3 process 160.

```
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] import-route ospfv3 160
```

Related commands

default-route-advertise (OSPFv3 view)

log-peer-change

Use **log-peer-change** to enable logging for neighbor state changes.

Use **undo log-peer-change** to disable logging for neighbor state changes.

Syntax

log-peer-change

undo log-peer-change

Default

Logging for neighbor state changes is enabled.

Views

OSPFv3 view

Predefined user roles

network-admin

Usage guidelines

This feature enables the device to deliver logs about neighbor state changes to its information center. The information center processes logs according to user-defined output rules (whether and where to output logs). For more information about the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Disable logging for neighbor state changes for OSPFv3 process 100.

```
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] undo log-peer-change
```

lsa-generation-interval

Use **lsa-generation-interval** to set the OSPFv3 LSA generation interval.

Use **undo lsa-generation-interval** to restore the default.

Syntax

lsa-generation-interval *maximum-interval* [*minimum-interval* [*incremental-interval*]]

undo lsa-generation-interval

Default

The maximum interval is 5 seconds, the minimum interval is 0 milliseconds, and the incremental interval is 0 milliseconds.

Views

OSPFv3 view

Predefined user roles

network-admin

Parameters

maximum-interval: Specifies the maximum OSPFv3 LSA generation interval in the range of 1 to 60 seconds.

minimum-interval: Specifies the minimum OSPFv3 LSA generation interval in the range of 10 to 60000 milliseconds. The default is 0, which indicates that the minimum interval can be any value.

incremental-interval: Specifies the OSPFv3 LSA generation incremental interval in the range of 10 to 60000 milliseconds.

Usage guidelines

When network changes are infrequent, LSAs are generated at the minimum interval. If network changes become frequent, the LSA generation interval is incremented by the incremental interval × 2^{n-2} for each generation until the maximum interval is reached. The value *n* is the number of generation times.

The minimum interval and the incremental interval cannot be greater than the maximum interval.

Examples

Set the maximum LSA generation interval to 2 seconds, minimum interval to 100 milliseconds, and incremental interval to 100 milliseconds.

```
<Sysname> system-view
[Sysname] ospfv3 100
```

```
[Sysname-ospfv3-100] lsa-generation-interval 2 100 100
```

Related commands

lsa-arrival-interval

non-stop-routing

Use **non-stop-routing** to enable OSPFv3 NSR.

Use **undo non-stop-routing** to disable OSPFv3 NSR.

Syntax

non-stop-routing

undo non-stop-routing

Default

OSPFv3 NSR is disabled.

Views

OSPFv3 view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only for the current process. As a best practice, enable OSPFv3 NSR for each process if multiple OSPFv3 processes exist.

OSPFv3 NSR and OSPFv3 GR are mutually exclusive. Do not configure the **non-stop-routing** command and the **graceful-restart enable** command at the same time.

Examples

Enable NSR for OSPFv3 process 100.

```
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] non-stop-routing
```

nssa (OSPFv3 area view)

Use **nssa** to configure an area as an NSSA area.

Use **undo nssa** to restore the default.

Syntax

nssa [**default-route-advertise** [**cost** *cost-value* | **nssa-only** | **route-policy** *route-policy-name* | **tag** *tag* | **type** *type*] * | **no-import-route** | **no-summary** | [**translate-always** | **translate-never**] | **suppress-fa** | **translator-stability-interval** *value*] *

undo nssa

Default

No area is configured as an NSSA area.

Views

OSPFv3 area view

Predefined user roles

network-admin

Parameters

default-route-advertise: Used on an NSSA ABR or an ASBR only. If it is configured on an NSSA ABR, the ABR redistributes a default route in a Type-7 LSA into the NSSA area. It redistributes a default route regardless of whether a default route exists in the routing table. If it is configured on an ASBR, the ASBR redistributes a default route in a Type-7 LSA only when the default route exists in the routing table.

cost *cost-value*: Specifies a cost for the default route, in the range of 0 to 16777214. If you do not specify this option, the default cost specified by the **default-cost** command applies.

nssa-only: Limits the default route advertisement to the NSSA area by setting the P-bit of Type-7 LSAs to 0. If you do not specify this keyword, the P-bit of Type-7 LSAs is set to 1. If the router acts as both an ASBR and an ABR and **FULL** state neighbors exist in the backbone area, the P-bit is set to 0.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters. When the specified routing policy is matched, the command redistributes a default route in a Type-7 LSA into the OSPFv3 routing domain. The routing policy modifies values in the Type-7 LSA.

tag *tag*: Specifies a tag for the default route, in the range of 0 to 4294967295.

type *type*: Specifies a type for the Type-7 LSA, 1 or 2. The default is 2.

no-import-route: Used on an NSSA ABR to control the **import-route** command to not redistribute routes into the NSSA area.

no-summary: Used only on an ABR to advertise a default route in a Type-3 summary LSA into the NSSA area and to not advertise other summary LSAs into the area. The area is a totally NSSA area.

translate-always: Always translates Type-7 LSAs to Type-5 LSAs. This keyword takes effect only on an NSSA ABR.

translate-never: Never translates Type-7 LSAs to Type-5 LSAs. This keyword takes effect only on an NSSA ABR.

suppress-fa: Suppresses the forwarding address in the Type-7 LSAs from being placed in the Type-5 LSAs.

translator-stability-interval *value*: Specifies the stability interval of the translator. During the interval, the translator can maintain its translating capability after another device becomes the new translator. The *value* argument is the stability interval in the range of 0 to 900 seconds. The default interval is 0. A value of 0 means the translator does not maintain its translating capability when a new translator arises.

Usage guidelines

All routers attached to an NSSA area must be configured with the **nssa** command in area view.

Examples

Configure Area 1 as an NSSA area.

```
<Sysname> system-view
[Sysname] ospfv3 120
[Sysname-ospfv3-120] area 1
[Sysname-ospfv3-120-area-0.0.0.1] nssa
```

Related commands

default-cost (OSPFv3 area view)

ospfv3

Use **ospfv3** to enable an OSPFv3 process and enter OSPFv3 view.

Use **undo ospfv3** to disable an OSPFv3 process.

Syntax

ospfv3 [*process-id*]

undo ospfv3 [*process-id*]

Default

No OSPFv3 process is enabled.

Views

System view

Predefined user roles

network-admin

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. The default process ID is 1.

Usage guidelines

Specify a router ID for the OSPFv3 process. Otherwise, the OSPFv3 process cannot generate LSAs.

Examples

Enable OSPFv3 process 120 and set the router ID to 1.1.1.1.

```
<Sysname> system-view
[Sysname] ospfv3 120
[Sysname-ospfv3-120] router-id 1.1.1.1
```

ospfv3 area

Use **ospfv3 area** to enable an OSPFv3 process on an interface and specify an area for the interface.

Use **undo ospfv3 area** to disable an OSPFv3 process on an interface.

Syntax

ospfv3 *process-id* **area** *area-id* [**instance** *instance-id*]

undo ospfv3 *process-id* **area** *area-id* [**instance** *instance-id*]

Default

No OSPFv3 processes are enabled on an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535.

area-id: Specifies an area by its ID, an IPv4 address or a decimal integer in the range of 0 to 4294967295 that is translated into the IPv4 address format.

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Examples

Configure VLAN-interface 10 to run instance 1 of OSPFv3 process 1 in Area 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 1 area 1 instance 1
```

ospfv3 authentication-mode

Use **ospfv3 authentication-mode** to specify an authentication mode for an OSPFv3 interface.

Use **undo ospfv3 authentication-mode** to remove the configuration.

Syntax

ospfv3 authentication-mode keychain *keychain-name* [**instance** *instance-id*]

undo ospfv3 authentication-mode [**instance** *instance-id*]

Default

No authentication is performed for an OSPFv3 interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

keychain: Specifies keychain authentication.

keychain-name: Specifies a keychain by its name, a case-sensitive string of 1 to 63 characters.

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

When keychain authentication is configured for an OSPFv3 interface, OSPFv3 performs the following operations before sending a packet:

1. Obtains a valid send key from the keychain.

   OSPFv3 does not send the packet if it fails to obtain a valid send key.
2. Uses the key ID, authentication algorithm, and key string to authenticate the packet.

   If the key ID is greater than 65535, OSPFv3 does not send the packet.

When keychain authentication is configured for an OSPFv3 interface, OSPFv3 performs the following operations after receiving a packet:

1. Uses the key ID carried in the packet to obtain a valid accept key from the keychain.

   OSPFv3 discards the packet if it fails to obtain a valid accept key.
2. Uses the authentication algorithm and key string for the valid accept key to authenticate the packet.

   If the authentication fails, OSPFv3 discards the packet.

OSPFv3 supports only the HMAC-SHA-256 authentication algorithm.

The ID of keys used for authentication can only be in the range of 0 to 65535.

Examples

Configure GigabitEthernet 1/0/1 to use the keychain **test** for OSPFv3 packet authentication.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospfv3 authentication-mode keychain test
```

ospfv3 bfd enable

Use **ospfv3 bfd enable** to enable BFD on an OSPFv3 interface.

Use **undo ospfv3 bfd enable** to disable BFD on an OSPFv3 interface.

Syntax

ospfv3 bfd enable [**instance** *instance-id*]

undo ospfv3 bfd enable [**instance** *instance-id*]

Default

BFD is disabled on an OSPFv3 interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

BFD provides a mechanism to quickly detect the connectivity of links between OSPFv3 neighbors, improving the convergence speed of OSPFv3.

OSPFv3 uses BFD to implement bidirectional control detection.

Examples

Enable BFD on VLAN-interface 11 in instance 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] ospfv3 bfd enable instance 1
```

ospfv3 cost

Use **ospfv3 cost** to set an OSPFv3 cost for an interface in an instance.

Use **undo ospfv3 cost** to remove the configuration.

Syntax

ospfv3 cost *cost-value* [**instance** *instance-id*]

undo ospfv3 cost [**instance** *instance-id*]

Default

The cost is 1 for a VLAN interface, is 0 for a loopback interface, and is computed according to the interface bandwidth for other interfaces.

Views

Interface view

Predefined user roles

network-admin

Parameters

cost-value: Specifies an OSPFv3 cost in the range of 0 to 65535 for a loopback interface, and in the range of 1 to 65535 for other interfaces.

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Examples

Set the OSPFv3 cost to 33 for VLAN-interface 10 in instance 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 cost 33 instance 1
```

ospfv3 dr-priority

Use **ospfv3 dr-priority** to set the router priority for an interface in an instance.

Use **undo ospfv3 dr-priority** to remove the configuration.

Syntax

ospfv3 dr-priority *priority* [**instance** *instance-id*]

undo ospfv3 dr-priority [**instance** *instance-id*]

Default

An interface has a router ID of 1.

Views

Interface view

Predefined user roles

network-admin

Parameters

priority: Specifies a router priority in the range of 0 to 255.

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

An interface's router priority determines its privilege in DR/BDR selection.

Examples

Set the router priority for VLAN-interface 10 in instance 1 to 8.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 dr-priority 8 instance 1
```

ospfv3 fast-reroute lfa-backup exclude

Use **ospfv3 fast-reroute lfa-backup exclude** to disable LFA on an interface.

Use **undo ospfv3 fast-reroute lfa-backup exclude** to remove the configuration.

Syntax

ospfv3 fast-reroute lfa-backup exclude [**instance** *instance-id*]

undo ospfv3 fast-reroute lfa-backup exclude [**instance** *instance-id*]

Default

LFA is enabled on an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

An interface enabled with LFA can be selected as a backup interface. After you disable LFA on the interface, it cannot be selected as a backup interface.

Examples

Disable VLAN-interface 11 from calculating a backup next hop by using the LFA algorithm.

```
<Sysname> system-view
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] ospfv3 fast-reroute lfa-backup exclude
```

ospfv3 ipsec-profile

Use **ospfv3 ipsec-profile** to apply an IPsec profile to an OSPFv3 interface.

Use **undo ospfv3 ipsec-profile** to remove the IPsec profile from the OSPFv3 interface.

Syntax

ospfv3 ipsec-profile *profile-name* [**instance** *instance-id*]

undo ospfv3 ipsec-profile [**instance** *instance-id*]

Default

No IPsec profile is applied to an OSPFv3 interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

profile-name: Specifies an IPsec profile by its name, a case-insensitive string of 1 to 63 characters.

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

An IPsec profile must be specified in this command. For more information about IPsec profiles, see *Security Configuration Guide*.

Examples

Apply IPsec profile **profile001** to VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 ipsec-profile profile001
```

ospfv3 mib-binding

Use **ospfv3 mib-binding** to bind an OSPFv3 process to MIB.

Use **undo ospfv3 mib-binding** to restore the default.

Syntax

ospfv3 mib-binding *process-id*

undo ospfv3 mib-binding

Default

MIB is bound to the OSPFv3 process with the smallest process ID.

Views

System view

Predefined user roles

network-admin

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535.

Usage guidelines

If the specified process ID does not exist, the MIB binding configuration fails.

Deleting an OSPFv3 process that has been bound to MIB unbinds the OSPFv3 process from MIB, and re-binds MIB to the OSPFv3 process with the smallest process ID.

Examples

Bind OSPFv3 process 100 to MIB.

```
<Sysname> system-view
[Sysname] ospfv3 mib-binding 100
```

ospfv3 mtu-ignore

Use **ospfv3 mtu-ignore** to configure an interface to ignore MTU check during DD packet exchange.

Use **undo ospfv3 mtu-ignore** to remove the configuration.

Syntax

ospfv3 mtu-ignore [**instance** *instance-id*]

undo ospfv3 mtu-ignore [**instance** *instance-id*]

Default

An interface performs MTU check during DD packet exchange.

Views

Interface view

Predefined user roles

network-admin

Parameters

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

A neighbor relationship can be established only if the interface's MTU is the same as that of the peer.

Examples

Configure VLAN-interface 10 that belongs to instance 1 to ignore MTU check during DD packet exchange.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 mtu-ignore instance 1
```

ospfv3 network-type

Use **ospfv3 network-type** to specify the network type for an OSPFv3 interface.

Use **undo ospfv3 network-type** to remove the configuration.

Syntax

ospfv3 network-type { **broadcast** | **nbma** | **p2mp** [**unicast**] | **p2p** } [**instance** *instance-id*]

undo ospfv3 network-type [**instance** *instance-id*]

Default

The network type of an OSPFv3 interface is broadcast.

Views

Interface view

Predefined user roles

network-admin

Parameters

broadcast: Specifies the network type as broadcast.

nbma: Specifies the network type as NBMA.

p2mp: Specifies the network type as P2MP.

unicast: Specifies the P2MP interface to unicast OSPFv3 packets. By default, a P2MP interface multicasts OSPFv3 packets.

p2p: Specifies the network type as P2P.

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

If a router on a broadcast network does not support multicast, configure the network type for the connected interfaces as NBMA.

When the network type of an interface is NBMA or P2MP unicast, you must use the **peer** command to specify the neighbor.

When the network type of an interface is P2MP unicast, all OSPFv3 packets are unicast by the interface.

Examples

Specify the OSPFv3 network type for VLAN-interface 20 as NBMA.

```
<Sysname> system-view
[Sysname] interface vlan-interface 20
[Sysname-Vlan-interface20] ospfv3 network-type nbma
```

Related commands

ospfv3 dr-priority

ospfv3 peer

Use **ospfv3 peer** to specify a neighbor and the DR priority of the neighbor.

Use **undo ospfv3 peer** to remove the configuration.

Syntax

ospfv3 peer *ipv6-address* [**cost** *cost-value* | **dr-priority** *priority*] [**instance** *instance-id*]

undo ospfv3 peer *ipv6-address* [**instance** *instance-id*]

Default

No link-local address is specified for the neighbor interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the link-local IPv6 address of the neighbor.

cost *cost-value*: Specifies the cost of the neighbor, in the range of 1 to 65535.

dr-priority *priority*: Specifies the DR priority of the neighbor, in the range of 0 to 255. The default is 1.

instance *instance-id:* Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

For NBMA and P2MP interfaces (only when in unicast mode), you must specify the link-local IPv6 addresses of their neighbors because these interfaces cannot find neighbors through broadcasting hello packets. For NBMA interfaces, you can also specify DR priorities for their neighbors.

Examples

On VLAN-interface 10, specify the link-local address of its neighbor as FE80::1111.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 peer fe80::1111
```

ospfv3 prefix-suppression

Use **ospfv3 prefix-suppression** to disable an OSPFv3 interface from advertising all its prefixes.

Use **undo ospfv3 prefix-suppression** to remove the configuration.

Syntax

ospfv3 prefix-suppression [**disable**] [**instance** *instance-id*]

undo ospfv3 prefix-suppression [**instance** *instance-id*]

Default

Prefix suppression is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

disable: Disables prefix suppression for an interface.

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

To disable prefix suppression for an interface associated with an OSPFv3 process that has been enabled with prefix suppression, use the **ospfv3 prefix-suppression disable** command on that interface.

Examples

Enable prefix suppression for VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 prefix-suppression
```

Related commands

prefix-suppression

ospfv3 primary-path-detect bfd

Use **ospfv3 primary-path-detect bfd** to enable BFD for OSPFv3 FRR.

Use **undo ospfv3 primary-path-detect bfd** to disable BFD for OSPFv3 FRR.

Syntax

ospfv3 primary-path-detect bfd { **ctrl** | **echo** } [**instance** *instance-id*]

undo ospfv3 primary-path-detect bfd [**instance** *instance-id*]

Default

BFD is disabled for OSPFv3 FRR.

Views

Interface view

Predefined user roles

network-admin

Parameters

ctrl: Enables BFD control packet mode.

echo: Enables BFD echo packet mode.

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

This command enables OSPFv3 FRR to use BFD to detect primary link failures.

Examples

On VLAN-interface 10, enable BFD echo packet mode for OSPFv3 FRR.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] fast-reroute lfa
[Sysname-ospfv3-1] quit
[Sysname] bfd echo-source-ipv6 1::1
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 primary-path-detect bfd echo
```

ospfv3 timer dead

Use **ospfv3 timer dead** to set the OSPFv3 neighbor dead time.

Use **undo ospfv3 timer dead** to remove the configuration.

Syntax

ospfv3 timer dead *seconds* [**instance** *instance-id*]

undo ospfv3 timer dead [**instance** *instance-id*]

Default

The OSPFv3 neighbor dead time is 40 seconds for P2P and broadcast interfaces, and is 120 seconds for P2MP and NBMA interfaces.

Views

Interface view

Predefined user roles

network-admin

Parameters

seconds: Specifies the dead time in the range of 1 to 65535 seconds.

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

If an interface receives no hello packet from a neighbor within the dead time, the interface determines that the neighbor is down.

The dead time must be a minimum of four times the hello time and must be identical on interfaces attached to the same network segment.

Examples

Set the OSPFv3 neighbor dead time to 60 seconds for VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 timer dead 60
```

Related commands

ospfv3 timer hello

ospfv3 timer hello

Use **ospfv3 timer hello** to set the hello interval for an interface.

Use **undo ospfv3 timer hello** to remove the configuration.

Syntax

ospfv3 timer hello *seconds* [**instance** *instance-id*]

undo ospfv3 timer hello [**instance** *instance-id*]

Default

The hello interval is 10 seconds for P2P and broadcast interfaces, and is 30 seconds for P2MP or NBMA interfaces.

Views

Interface view

Predefined user roles

network-admin

Parameters

seconds: Specifies the hello interval in the range of 1 to 65535 seconds.

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

The shorter the hello interval is, the faster the topology converges and the more resources are consumed. Make sure the hello interval on two neighboring interfaces is the same.

Examples

Set the hello interval to 20 seconds for VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 timer hello 20
```

Related commands

ospfv3 timer dead

ospfv3 timer poll

Use **ospfv3 timer poll** to set the poll interval on an NBMA interface.

Use **undo ospfv3 timer poll** to remove the configuration.

Syntax

ospfv3 timer poll *seconds* [**instance** *instance-id*]

undo ospfv3 timer poll [**instance** *instance-id*]

Default

The poll interval is 120 seconds on an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

seconds: Specifies the poll interval in the range of 1 to 65535 seconds.

instance *instance-id*: Specifies an interface instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

When an NBMA interface finds its neighbor is down, it sends hello packets at the poll interval.

The poll interval must be a minimum of four times the hello interval.

Examples

Set the poll interval on VLAN-interface 10 to 120 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 timer poll 120
```

Related commands

ospfv3 timer hello

ospfv3 timer retransmit

Use **ospfv3 timer retransmit** to set the LSA retransmission interval for an interface.

Use **undo ospfv3 timer retransmit** to remove the configuration.

Syntax

ospfv3 timer retransmit *seconds* [**instance** *instance-id*]

undo ospfv3 timer retransmit [**instance** *instance-id*]

Default

The interval is 5 seconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

seconds: Specifies the LSA retransmission interval in the range of 1 to 3600 seconds.

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

After the device sends an LSA to its neighbor, it waits for an acknowledgment. If the device receives no acknowledgment after the LSA retransmission interval elapses, it will retransmit the LSA.

To avoid unnecessary retransmissions, set an appropriate retransmission interval. For example, you can set a large retransmission interval value on a low-speed link.

Examples

Set the LSA retransmission interval to 12 seconds on VLAN-interface10 in instance 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 timer retransmit 12 instance 1
```

ospfv3 trans-delay

Use **ospfv3 trans-delay** to set the transmission delay for an interface.

Use **undo ospfv3 trans-delay** to remove the configuration.

Syntax

ospfv3 trans-delay *seconds* [**instance** *instance-id*]

undo ospfv3 trans-delay [**instance** *instance-id*]

Default

The transmission delay is 1 second.

Views

Interface view

Predefined user roles

network-admin

Parameters

seconds: Specifies the transmission delay in the range of 1 to 3600 seconds.

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

Each LSA in the LSDB has an age that is incremented by 1 every second, but the age does not change during transmission. Adding a transmission delay into the age time is important in low speed networks.

Examples

Set the transmission delay to 3 seconds for VLAN-interface 10 in instance 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 trans-delay 3 instance 1
```

preference

Use **preference** to set a preference for OSPFv3 routes.

Use **undo preference** to remove the configuration.

Syntax

preference [**ase**] { *preference* | **route-policy** *route-policy-name* } *

undo preference [**ase**]

Default

The preference is 10 for OSPFv3 internal routes and 150 for OSPFv3 external routes.

Views

OSPFv3 view

Predefined user roles

network-admin

Parameters

ase: Specifies a preference for OSPFv3 external routes. If you do not specify this keyword, the command sets a preference for OSPFv3 internal routes.

preference: Specifies the preference value in the range of 1 to 255. A smaller value represents a higher preference.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to set a preference for matching routes.

Usage guidelines

If multiple routing protocols find multiple routes to the same destination, the router uses the route found by the protocol with the highest preference.

Examples

Set a preference of 150 for OSPFv3 routes.

```
<Sysname> system-view
[Sysname] OSPFv3
[Sysname-OSPFv3-1] preference 150
```

prefix-suppression

Use **prefix-suppression** to disable an OSPFv3 process from advertising all prefixes except for the prefixes of loopback interfaces and passive interfaces.

Use **undo prefix-suppression** to restore the default.

Syntax

prefix-suppression

undo prefix-suppression

Default

An OSPFv3 process advertises all prefixes.

Views

OSPFv3 view

Predefined user roles

network-admin

Usage guidelines

By default, an OSPFv3 interface advertises all of its prefixes in LSAs. To speed up OSPFv3 convergence, you can suppress interfaces from advertising all of their prefixes. This feature helps improve network security by preventing IP routing to the suppressed networks.

To disable an OSPFv3 process from advertising the prefixes of loopback and passive interfaces, configure prefix suppression on the interfaces by using the **ospfv3 prefix-suppression** command.

When prefix suppression is enabled:

- OSPFv3 does not advertise the prefixes of suppressed interfaces in Type-8 LSAs.
- On broadcast and NBMA networks, the DR does not advertise the prefixes of suppressed interfaces in Type-9 LSAs that reference Type-2 LSAs.
- On P2P and P2MP networks, OSPFv3 does not advertise the prefixes of suppressed interfaces in Type-9 LSAs that reference Type-1 LSAs.

Examples

Enable prefix suppression for OSPFv3 process 100.

```
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] prefix-suppression
```

Related commands

ospfv3 prefix-suppression

reset ospfv3 event-log

Use **reset ospfv3 event-log** to clear OSPFv3 log information.

Syntax

reset ospfv3 [*process-id*] **event-log** [**lsa-flush** | **peer** | **spf**]

Views

User view

Predefined user roles

network-admin

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command clears OSPFv3 log information for all OSPFv3 processes.

lsa-flush: Clears LSA aging log information.

peer: Clears neighbor log information.

spf: Clears route calculation log information.

Usage guidelines

If you do not specify a log type, this command clears all log information.

Examples

Clear OSPFv3 route calculation log information for all OSPFv3 processes.

```
<Sysname> reset ospfv3 event-log spf
```

Related commands

display ospfv3 event-log

reset ospfv3 process

Use **reset ospfv3 process** to restart OSPFv3 processes.

Syntax

reset ospfv3 [*process-id*] **process** [**graceful-restart**]

Views

User view

Predefined user roles

network-admin

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command restarts all OSPFv3 processes.

graceful-restart: Restarts the OSPFv3 process by using GR.

Usage guidelines

The **reset ospfv3 process** command performs the following actions:

- Clears all invalid LSAs without waiting for their timeouts.
- Starts a new DR/BDR election.
- Keeps previous OSPFv3 configurations.

The system prompts you to select whether to restart OSPFv3 process upon execution of this command.

Examples

Restart all OSPFv3 processes.

```
<Sysname> reset ospfv3 process
Reset OSPFv3 process? [Y/N]:y
```

reset ospfv3 redistribution

Use **reset ospfv3 redistribution** to restart route redistribution.

Syntax

reset ospfv3 [*process-id*] **redistribution**

Views

User view

Predefined user roles

network-admin

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command restarts route redistribution for all OSPFv3 processes.

Examples

Restart route redistribution.

```
<Sysname> reset ospfv3 redistribution
```

reset ospfv3 statistics

Use **reset ospfv3 statistics** to clear OSPFv3 statistics.

Syntax

reset ospfv3 [*process-id*] **statistics**

Views

User view

Predefined user roles

network-admin

Parameters

process-id: Specifies an OSPFv3 process by its ID in the range of 1 to 65535. If you do not specify this argument, the command clears statistics for all OSPFv3 processes.

Examples

Clear statistics for all OSPFv3 processes.

```
<Sysname> reset ospfv3 statistics
```

router-id

Use **router-id** to configure a router ID.

Use **undo router-id** to restore the default.

Syntax

router-id *router-id*

undo router-id

Default

No router ID is configured.

Views

OSPFv3 view

Predefined user roles

network-admin

Parameters

router-id: Specifies a router ID in IPv4 address format.

Usage guidelines

The router ID is the unique identifier for the device to run OSPFv3 in the AS. An OSPFv3 process cannot run without a router ID.

You must specify a unique router ID for each OSPFv3 process in an AS and on a router.

Examples

Configure the router ID 10.1.1.3 for OSPFv3 process 1.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] router-id 10.1.1.3
```

Related commands

ospfv3

silent-interface(OSPFv3 view)

Use **silent-interface** to disable the specified interface from receiving and sending OSPFv3 packets.

Use **undo silent-interface** to remove the configuration.

Syntax

silent-interface { *interface-type interface-number* | **all** }

undo silent-interface { *interface-type interface-number* | **all** }

Default

An interface can receive and send OSPFv3 packets.

Views

OSPFv3 view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

all: Specifies all interfaces.

Usage guidelines

Multiple processes can disable the same interface from receiving and sending OSPFv3 packets. However, the **silent-interface** command takes effect only on interfaces enabled with the current process.

Examples

Disable VLAN-interface 10 from receiving and sending OSPFv3 packets in OSPFv3 processes 100 and 200.

```
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] router-id 10.100.1.9
[Sysname-ospfv3-100] silent-interface vlan-interface 10
[Sysname-ospfv3-100] quit
[Sysname] ospfv3 200
[Sysname-ospfv3-200] router-id 20.100.1.9
[Sysname-ospfv3-200] silent-interface vlan-interface 10
```

snmp context-name

Use **snmp context-name** to configure an SNMP context for OSPFv3.

Use **undo snmp context-name** to restore the default.

Syntax

snmp context-name *context-name*

undo snmp context-name

Default

No SNMP contexts exist for OSPFv3.

Views

OSPFv3 view

Predefined user roles

network-admin

Parameters

context-name: Specifies a context name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

The standard OSPFv3 MIB provides only single-instance MIB objects. For SNMP to correctly identify OSPFv3 management information in the standard OSPFv3 MIB, you must configure a unique context name for OSPFv3. If multiple OSPFv3 processes exist, you must assign a unique context to each process.

Context is a method introduced to SNMPv3 for multiple-instance management. For SNMPv1/v2c, you must specify a community name as a context name for protocol identification.

Examples

Configure the SNMP context name as **mib** for OSPFv3 process 1.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] snmp context-name mib
```

snmp trap rate-limit

Use **snmp trap rate-limit** to set the SNMP notification output interval and the maximum number of SNMP notifications that can be output at each interval.

Use **undo snmp trap rate-limit** to restore the default.

Syntax

snmp trap rate-limit interval *trap-interval* **count** *trap-number*

undo snmp trap rate-limit

Default

OSPFv3 outputs a maximum of seven SNMP notifications within 10 seconds.

Views

OSPFv3 view

Predefined user roles

network-admin

Parameters

interval *trap-interval*: Specifies the SNMP notification output interval in the range of 2 to 60 seconds.

count *trap-number*: Specifies the number of SNMP notifications output by OSPFv3 at each interval, in the range of 0 to 300. The value of 0 indicates that OSPFv3 does not output SNMP notifications.

Examples

Configure OSPFv3 to output a maximum of 10 SNMP notifications within 5 seconds.

```
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] snmp trap rate-limit interval 5 count 10
```

snmp-agent trap enable ospfv3

Use **snmp-agent trap enable ospfv3** to enable SNMP notifications for OSPFv3.

Use **undo snmp-agent trap enable ospfv3** to disable SNMP notifications for OSPFv3.

Syntax

snmp-agent trap enable ospfv3 [**grrestarter-status-change** | **grhelper-status-change** | **if-state-change** | **if-cfg-error** | **if-bad-pkt** | **neighbor-state-change** | **nssatranslator-status-change** | **virtif-bad-pkt** | **virtif-cfg-error** | **virtif-state-change** | **virtgrhelper-status-change** | **virtneighbor-state-change**] *

undo snmp-agent trap enable ospfv3 [**grrestarter-status-change** | **grhelper-status-change** | **if-state-change** | **if-cfg-error** | **if-bad-pkt** | **neighbor-state-change** | **nssatranslator-status-change** | **virtif-bad-pkt** | **virtif-cfg-error** | **virtif-state-change** | **virtgrhelper-status-change** | **virtneighbor-state-change**] *

Default

SNMP notifications for OSPFv3 are enabled.

Views

System view

Predefined user roles

network-admin

Parameters

grrestarter-status-change: Specifies notifications about GR restarter state changes.

grhelper-status-change: Specifies notifications about GR helper state changes.

if-state-change: Specifies notifications about interface state changes.

if-cfg-error: Specifies notifications about error configuration of an interface.

if-bad-pkt: Specifies notifications about error messages received on an interface.

neighbor-state-change: Specifies notifications about neighbor state changes.

nssatranslator-status-change: Specifies notifications about NSSA translator state changes.

virtif-bad-pkt: Specifies notifications about error messages received on a virtual interface.

virtif-cfg-error: Specifies notifications about error configuration of a virtual interface.

virtif-state-change: Specifies notifications about virtual interface state changes.

virtgrhelper-status-change: Specifies notifications about neighbor GR helper state changes of a virtual interface.

virtneighbor-state-change: Specifies notifications about the neighbor state changes of a virtual interface.

Examples

Disable SNMP notifications for OSPFv3.

```
<Sysname> system-view
[Sysname] undo snmp-agent trap enable ospfv3
```

spf-schedule-interval

Use **spf-schedule-interval** to set the OSPFv3 SPF calculation interval.

Use **undo spf-schedule-interval** to restore the default.

Syntax

spf-schedule-interval *maximum-interval* [*minimum-interval* [*incremental-interval*]]

undo spf-schedule-interval

Default

The maximum SPF calculation interval is 5 seconds, the minimum interval is 50 milliseconds, and the incremental interval is 200 milliseconds.

Views

OSPFv3 view

Predefined user roles

network-admin

Parameters

maximum-interval: Specifies the maximum OSPFv3 route calculation interval in the range of 1 to 60 seconds.

minimum-interval: Specifies the minimum OSPFv3 route calculation interval in the range of 10 to 60000 milliseconds.

incremental-interval: Specifies the incremental OSPFv3 route calculation interval in the range of 10 to 60000 milliseconds.

Usage guidelines

Based on the LSDB, an OSPFv3 router uses SPF to calculate a shortest path tree with itself being the root. OSPFv3 uses the shortest path tree to determine the next hop to a destination. By adjusting the SPF calculation interval, you can prevent overconsumption of bandwidth and router resources due to frequent topology changes.

For a stable network, the minimum interval is used. If network changes become frequent, the SPF calculation interval is incremented by the incremental interval × 2^{n-2} for each calculation until the maximum interval is reached. The value *n* is the number of calculation times.

The minimum interval and the incremental interval cannot be greater than the maximum interval.

Examples

Set the maximum SPF calculation interval to 10 seconds, minimum interval to 500 milliseconds, and incremental interval to 300 milliseconds.

```
<Sysname> system-view
```

```
[Sysname] ospfv3 100
[Sysname-ospfv3-100] spf-schedule-interval 10 500 300
```

stub (OSPFv3 area view)

Use **stub** to configure an area as a stub area.

Use **undo stub** to restore the default.

Syntax

stub [**default-route-advertise-always** | **no-summary**] *

undo stub

Default

No area is configured as a stub area.

Views

OSPFv3 area view

Predefined user roles

network-admin

Parameters

default-route-advertise-always: Enables the ABR to always advertise a default route into the stub area.

no-summary: Enables the ABR to advertise only a default route in an Inter-Area-Prefix-LSA into the stub area. No AS-external-LSA, Inter-Area-Prefix-LSA, or other Inter-Area-Router-LSA is advertised in the area. The area is a totally stub area.

Usage guidelines

To remove the **no-summary** configuration on an ABR, execute the **stub** command again to overwrite it.

To configure an area as a stub area, execute the **stub** command on all routers attached to the area.

Examples

Configure OSPFv3 area 1 as a stub area.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 1
[Sysname-ospfv3-1-area-0.0.0.1] stub
```

Related commands

default-cost (OSPFv3 area view)

stub-router

Use **stub-router** to configure a router as a stub router.

Use **undo stub-router** to restore the default.

Syntax

stub-router r-bit [**include-stub** | **on-startup** *seconds*] *

stub-router max-metric [**external-lsa** [*max-metric-value*] | **summary-lsa** [*max-metric-value*] | **include-stub** | **on-startup** *seconds*] *

undo stub-router

Default

The router is not configured as a stub router.

Views

OSPFv3 view

Predefined user roles

network-admin

Parameters

r-bit: Clears the R-bit of the Option field in Type-1 LSAs.

max-metric: Advertises the locally generated Type-1 LSAs with the maximum cost of 65535.

external-lsa *max-metric-value*: Specifies a cost for external LSAs, in the range of 1 to 16777215. The default is 16711680.

summary-lsa *max-metric-value*: Specifies a cost for Type-3 and Type-4 LSAs, in the range of 1 to 16777215. The default is 16711680.

include-stub: Specifies the cost for Type-9 LSAs that reference Type-1 LSAs to the maximum value 65535.

on-startup *seconds*: Specifies the router as a stub router during reboot, and specifies the timeout time in the range of 5 to 86400 seconds.

Usage guidelines

You can use the **stub-router r-bit** command or **stub-router max-metric** command to configure a router as a stub router.

- The **stub-router r-bit** command clears the R-bit of the Option field in Type-1 LSAs. When the R-bit is clear, the OSPFv3 router can participate in OSPFv3 topology distribution without forwarding traffic.
- The **stub-router max-metric** command specifies the OSPFv3 max-metric router LSA feature. This feature enables OSPFv3 to advertise its locally generated Type-1 LSAs with a maximum cost of 65535. Neighbors do not send packets to the stub router as long as they have a route with a smaller cost.

Examples

Configure a stub router.

```
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] stub-router r-bit
```

transmit-pacing

Use **transmit-pacing** to set the LSU transmission interval and the maximum number of LSU packets that can be sent at each interval.

Use **undo transmit-pacing** to restore the default.

Syntax

transmit-pacing interval *interval* **count** *count*

undo transmit-pacing

Default

An OSPFv3 interface sends a maximum of three LSU packets every 20 milliseconds.

Views

OSPFv3 view

Predefined user roles

network-admin

Parameters

interval *interval*: Specifies an interval at which an interface sends LSU packets, in the range of 10 to 1000 milliseconds. If the router has multiple OSPFv3 interfaces, increase the interval to reduce the total number of LSU packets sent by the router every second.

count *count*: Specifies the maximum number of LSU packets sent by an interface at each interval, in the range of 1 to 200. If the router has multiple OSPFv3 interfaces, decrease the maximum number to reduce the total number of LSU packets sent by the router every second.

Examples

Configure all the interfaces running OSPFv3 process 1 to send a maximum of 10 LSU packets every 30 milliseconds.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] transmit-pacing interval 30 count 10
```

vlink-peer (OSPFv3 area view)

Use **vlink-peer** to configure a virtual link.

Use **undo vlink-peer** to remove a virtual link.

Syntax

vlink-peer *router-id* [**dead** *seconds* | **hello** *seconds* | **instance** *instance-id* | **ipsec-profile** *profile-name* | **keychain** *keychain-name* | **retransmit** *seconds* | **trans-delay** *seconds*] *

undo vlink-peer *router-id* [**dead** | **hello** | **ipsec-profile** | **retransmit** | **trans-delay**] *

Default

No virtual links exist.

Views

OSPFv3 area view

Predefined user roles

network-admin

Parameters

router-id: Specifies the router ID of the neighbor on the virtual link.

dead *seconds*: Specifies the dead interval in the range of 1 to 32768 seconds. The default is 40. The dead interval must be identical with that on the virtual link neighbor, and must be a minimum of four times the hello interval.

hello *seconds*: Specifies the hello interval in the range of 1 to 8192 seconds. The default is 10. It must be identical with the hello interval on the virtual link neighbor.

instance *instance-id*: Specifies the instance ID of a virtual link, in the range of 0 to 255. The default is 0.

ipsec-profile *profile-name:* Specifies an IPsec profile by its name, a case-insensitive string of 1 to 63 characters. For more information about IPsec profiles, see *Security Configuration Guide*.

keychain: Specifies the keychain authentication mode.

keychain-name: Specifies a keychain by its name, a case-sensitive string of 1 to 63 characters.

retransmit *seconds*: Specifies the retransmission interval in the range of 1 to 3600 seconds. The default is 5.

trans-delay *seconds*: Specifies the transmission delay interval in the range of 1 to 3600 seconds. The default is 1.

Usage guidelines

You can configure a virtual link to maintain connectivity between a non-backbone area and the backbone, or maintain connectivity within the backbone. A virtual link is similar to an interface with OSPFv3 enabled. You can configure parameters such as **hello**, **dead**, **retransmit** and **trans-delay** for the virtual link.

Both ends of a virtual link must be ABRs that are configured with the **vlink-peer** command.

The following guidelines apply to parameters:

- The smaller the hello interval is, the faster the network converges, and the more network resources are consumed.
- For a low speed link, set a large retransmission interval to avoid unnecessary retransmissions.
- Specify a transmission delay with the **trans-delay** keyword depending on the interface delay.

The authentication mode specified for an OSPFv3 virtual link has a higher priority than the mode specified for the backbone area. If no authentication mode is specified for the virtual link, the mode specified for the backbone area applies.

When keychain authentication is configured for an OSPFv3 virtual link, OSPFv3 performs the following operations before sending a packet:

1. Obtains a valid send key from the keychain.

   OSPFv3 does not send the packet if it fails to obtain a valid send key.
2. Uses the key ID, authentication algorithm, and key string to authenticate the packet.

   If the key ID is greater than 65535, OSPFv3 does not send the packet.

When keychain authentication is configured for an OSPFv3 virtual link, OSPFv3 performs the following operations after receiving a packet:

1. Uses the key ID carried in the packet to obtain a valid accept key from the keychain.

   OSPFv3 discards the packet if it fails to obtain a valid accept key.
2. Uses the authentication algorithm and key string for the valid accept key to authenticate the packet.

   If the authentication fails, OSPFv3 discards the packet.

OSPFv3 supports only the HMAC-SHA-256 authentication algorithm.

The ID of keys used for authentication can only be in the range of 0 to 65535.

Examples

Configure a virtual link to 10.10.0.3.

```
<Sysname> system-view
[Sysname] ospfv3 1
```

```
[Sysname-ospfv3-1] area 1
[Sysname-ospfv3-1-area-0.0.0.1] vlink-peer 10.10.0.3
```

Related commands

display ospfv3 vlink

Contents

IPv6 policy-based routing commands

apply next-hop

Use **apply next-hop** to set next hops.

Use **undo apply next-hop** to remove next hops.

Syntax

apply next-hop { *ipv6-address* [**direct**] [**track** *track-entry-number*] } &<1-2>

undo apply next-hop [*ipv6-address*&<1-2>]

Default

No next hops are set.

Views

IPv6 policy node view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the IPv6 address of the next hop.

direct: Specifies that the next hop must be directly connected to take effect.

track *track-entry-number*: Specifies a track entry by its number in the range of 1 to 1024.

&<1-2>: Indicates that the argument before it can be entered up to two times.

Usage guidelines

You can specify multiple next hops for backup in one command line or by executing this command multiple times.

With a next hop specified, the **undo apply next-hop** command removes the next hop.

Without any next hop specified, the **undo apply next-hop** command removes all next hops.

Examples

Set a directly-connected next hop of 1::1.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 11
[Sysname-pbr6-aa-11] apply next-hop 1::1
```

description

Use **description** to configure a description for an IPv6 policy node.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

No description is configured for an IPv6 policy node.

Views

IPv6 policy node view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 127 characters.

Examples

Configure the description as **Officeuse** for IPv6 policy node 1.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route 1 permit node 1
[Sysname-pbr6-1-1] description Officeuse
```

display ipv6 policy-based-route

Use **display ipv6 policy-based-route** to display IPv6 PBR policy information.

Syntax

display ipv6 policy-based-route [**policy** *policy-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

policy *policy-name*: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters. If you do not specify a policy, this command displays information for all IPv6 PBR policies.

Examples

Display all IPv6 policy information.

```
<Sysname> display ipv6 policy-based-route
Policy name: aaa
  node 1 permit:
    if-match acl 2000
    apply next-hop 1000::1
```

Table 1 Command output

Field	Description
node 1 permit	The match mode of Node 1 is **permit**.
if-match acl	Compares IPv6 packets with IPv6 ACL.
apply next-hop	Specifies a next hop for permitted IPv6 packets.

Related commands

ipv6 policy-based-route (system view)

display ipv6 policy-based-route interface

Use **display ipv6 policy-based-route interface** to display IPv6 interface PBR configuration and statistics.

Syntax

display ipv6 policy-based-route interface *interface-type interface-number* [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 interface PBR configuration and statistics for the master device.

Examples

Display IPv6 PBR configuration and statistics on VLAN-interface 2.

```
<Sysname> display ipv6 policy-based-route interface vlan-interface 2
Policy based routing information for interface Vlan-inerface2(failed):
Policy name: aaa
  node 0 deny:
  Matched: 0
  node 1 permit:
    if-match acl 3999
  Matched: 0
  node 2 permit:
    if-match acl 2000
    apply next-hop 1000::1
  Matched: 0
  node 5 permit:
    if-match acl 3101
    apply next-hop 1000::1
  Matched: 0
Total matched: 0
<Sysname> display ipv6 policy-based-route interface Vlan-inerface2
Policy based routing information for interface Vlan-inerface2:
Policy name: aaa
  node 0 deny(not support):
  Matched: 0
  node 1 permit:
```

```
    if-match acl 3999
  Matched: 0
  node 2 permit(no resource):
    if-match acl 2000
    apply next-hop 1000::1
  Matched: 0
  node 5 permit:
    if-match acl 3101
    apply next-hop 1000::1
  Matched: 0 (no statistics resource)
Total matched: 0
```

Table 2 Command output

Field	Description
Policy based routing information for interface *XXXX* (failed)	IPv6 PBR configuration and statistics on the interface. This field displays **failed** in brackets if none of the nodes in the policy has been successfully issued to the driver. The **failed** status will persist even after the policy is successfully issued. To clear the **failed** status, you must remove the policy from the interface and then apply it on the interface again. **NOTE:** The **failed** status is available on a per-slot basis. To obtain this information, you must specify a slot number when you execute the command. • For a global interface (for example, a VLAN interface), which might have member physical interfaces on multiple slots, specify a slot that contains its member interfaces. • For a physical interface, specify its slot number.
node 0 deny(not support) node 2 permit(no resource)	Match mode of the node, **permit** or **deny**. If a node fails to be issued to the driver, the command displays the cause in brackets, which include: • **not support**—The device does not support the match criteria configured on the node. • **no resource**—No sufficient resources (for example, ACLs) are available for the node. **NOTE:** The cause is available only on a per-slot basis. To obtain this information, you must specify a slot number when you execute the command. • For a global interface (for example, a VLAN interface), which might have member physical interfaces on multiple slots, specify a slot that contains its member interfaces. • For a physical interface, specify its slot number.
if-match acl	Compares IPv6 packets with the IPv6 ACL.
apply next-hop	Specifies a next hop for permitted IPv6 packets.
Matched: 0 (no statistics resource)	Number of successful matches on the node. If the device does not have sufficient resources to count matches, this field displays **no statistics resource** in brackets. **NOTE:** The statistics collection failure cause is available only on a per-slot basis. To obtain this information, you must specify a slot number when you execute the command.

Field	Description
	• For a global interface (for example, a VLAN interface), which might have member physical interfaces on multiple slots, specify a slot that contains its member interfaces. • For a physical interface, specify its slot number.
Total matched	Total number of successful matches on all nodes.

Related commands

reset ipv6 policy-based-route statistics

display ipv6 policy-based-route local

Use **display ipv6 policy-based-route local** to display IPv6 local PBR configuration and statistics.

Syntax

display ipv6 policy-based-route local [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 local PBR configuration and statistics for the master device.

Examples

Display IPv6 local PBR configuration and statistics.

```
<Sysname> display ipv6 policy-based-route local
Policy based routing information for local:
Policy name: aaa
  node 0 deny:
  Matched: 0
  node 1 permit:
    if-match acl 3999
  Matched: 0
  node 2 permit:
    if-match acl 2000
    apply next-hop 1::1
  Matched: 0
  node 5 permit:
    if-match acl 3101
    apply next-hop 2::2
  Matched: 0
Total matched: 0
```

Table 3 Command output

Field	Description
Policy based routing information for local	IPv6 local PBR configuration and statistics.
node 0 deny/node 2 permit	Match mode of the node, **permit** or **deny**.
if-match acl	Compares packets with the ACL.
apply next-hop	Specifies a next hop for permitted packets.
Matched: 0	Number of successful matches on the node.
Total matched	Total number of successful matches on all nodes.

Related commands

`reset ipv6 policy-based-route statistics`

display ipv6 policy-based-route setup

Use **`display ipv6 policy-based-route setup`** to display IPv6 PBR configuration.

Syntax

`display ipv6 policy-based-route setup`

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display IPv6 PBR configuration.

```
<Sysname> display ipv6 policy-based-route setup
Policy name             Type               Interface
pr01                    Forward            Vlan-interface 2
pr02                    Local              N/A
pr03                    Global             N/A
```

Table 4 Command output

Field	Description
Policy name	Policy name.
Type	Type of the PBR: • **Forward**—Interface PBR. • **Local**—Local PBR. • **Global**—Global PBR.
Interface	Interface where the policy is applied. This field displays **N/A** for IPv6 local PBR and IPv6 global PBR.

Related commands

ipv6 policy-based-route (interface view)

if-match acl

Use **if-match acl** to set an ACL match criterion.

Use **undo if-match acl** to restore the default.

Syntax

if-match acl { *ipv6-acl-number* | **name** *ipv6-acl-name* }

undo if-match acl

Default

No ACL match criterion is set.

Views

IPv6 policy node view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies an IPv6 ACL by its number in the range of 2000 to 3999. The value range of a basic ACL is 2000 to 2999 and that of an advanced ACL is 3000 to 3999.

name *ipv6-acl-name*: Specifies an IPv6 ACL by its name, a case-insensitive string of 1 to 63 characters starting with a letter. The ACL name cannot be **all**. For the command to take effect, make sure the specified IPv6 ACL is a basic or advanced ACL.

Examples

Configure Node 10 of policy **aa** to permit the packets matching ACL 2000.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 10
[Sysname-pbr6-aa-10] if-match acl 2000
```

Configure Node 10 of policy **aa** to permit the packets matching ACL **aaa**.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 10
[Sysname-pbr6-aa-10] if-match acl name aaa
```

ipv6 local policy-based-route

Use **ipv6 local policy-based-route** to configure IPv6 local PBR based on a specified policy.

Use **undo ipv6 local policy-based-route** to restore the default.

Syntax

ipv6 local policy-based-route *policy-name*

undo ipv6 local policy-based-route

Default

No policy is referenced for IPv6 local PBR.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters. The specified IPv6 policy must already exist.

Usage guidelines

You can apply only one policy locally. Before you apply a new policy, you must first remove the current policy.

IPv6 local PBR is used to route locally generated packets except the packets destined for the sender. This feature might affect local services. Do not configure IPv6 local PBR unless doing so is required.

Examples

Configure IPv6 local PBR based on policy **aaa**.

```
<Sysname> system-view
[Sysname] ipv6 local policy-based-route aaa
```

Related commands

display ipv6 policy-based-route setup

ipv6 policy-based-route (system view)

ipv6 policy-based-route (interface view)

Use **ipv6 policy-based-route** to configure IPv6 interface PBR by applying an IPv6 policy to an interface.

Use **undo ipv6 policy-based-route** to restore the default.

Syntax

ipv6 policy-based-route *policy-name*

undo ipv6 policy-based-route

Default

No IPv6 policy is applied to an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters. The specified policy must already exist.

Examples

Apply policy **aaa** to VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ipv6 policy-based-route aaa
```

Related commands

display ipv6 policy-based-route setup

ipv6 policy-based-route (system view)

ipv6 policy-based-route (system view)

Use **ipv6 policy-based-route** to create an IPv6 policy node and enter its view, or enter the view of an existing IPv6 policy node.

Use **undo ipv6 policy-based-route** to delete an IPv6 policy or IPv6 policy node.

Syntax

ipv6 policy-based-route *policy-name* [**deny** | **permit**] **node** *node-number*

undo ipv6 policy-based-route *policy-name* [**deny** | **node** *node-number* | **permit**]

Default

No IPv6 policy nodes exist.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a policy name, a case-sensitive string of 1 to 19 characters.

deny: Specifies the match mode for the policy node as **deny**.

permit: Specifies the match mode for the policy node as **permit** (default mode).

node *node-number*: Specifies the number of the IPv6 policy node. A smaller number has a higher priority. The value range for the *node-number* argument is 0 to 255.

Usage guidelines

To delete an IPv6 policy that has already applied to an interface, you must delete the policy from the interface first.

If a policy node is specified, the **undo ipv6 policy-based-route** command deletes the specified policy node. If a match mode is specified, the command deletes all nodes configured with the match mode. If no node is specified, the command deletes the whole policy.

Examples

Create permit-mode Node 10 for IPv6 policy **aaa** and enter its view.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aaa permit node 10
[Sysname-pbr6-aaa-10]
```

Related commands

display ipv6 policy-based-route

reset ipv6 policy-based-route statistics

Use **reset ipv6 policy-based-route statistics** to clear IPv6 PBR statistics.

Syntax

reset ipv6 policy-based-route statistics [**policy** *policy-name*]

Views

User view

Predefined user roles

network-admin

Parameters

policy *policy-name*: Specifies a policy by its name, a case-sensitive string of 1 to 19 characters. If you do not specify a policy, this command clears IPv6 PBR statistics for all policies.

Examples

Clear all IPv6 PBR statistics.

```
<Sysname> reset ipv6 policy-based-route statistics
```

Related commands

display ipv6 policy-based-route interface

display ipv6 policy-based-route local

Contents

Routing policy commands

Common routing policy commands

apply cost

Use **apply cost** to set a cost for routes.

Use **undo apply cost** to restore the default.

Syntax

apply cost [**+** | **-**] *cost-value*

undo apply cost

Default

No cost is set for routes.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

+: Increases a cost value.

-: Decreases a cost value.

cost-value: Specifies a cost in the range of 0 to 4294967295.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to set a cost of 120 for OSPF external routes.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match route-type external-type1or2
[Sysname-route-policy-policy1-10] apply cost 120
```

apply cost-type

Use **apply cost-type** to set a cost type for routes.

Use **undo apply cost-type** to restore the default.

Syntax

apply cost-type { **type-1** | **type-2** }

undo apply cost-type

Default

No cost type is set for routes.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

type-1: Sets the cost type to OSPF Type-1 external route.

type-2: Sets the cost type to OSPF Type-2 external route.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to set the cost type for routes that have a tag of 8 to OSPF Type-1 external routes.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match tag 8
[Sysname-route-policy-policy1-10] apply cost-type type-1
```

apply ip-precedence

Use **apply ip-precedence** to set an IP precedence for matching routes.

Use **undo apply ip-precedence** to restore the default.

Syntax

apply ip-precedence { *value* | **clear** }

undo apply ip-precedence

Default

No IP precedence is set.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

value: Specifies an IP precedence in the range of 0 to 7.

clear: Clears the IP precedence of matching routes.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to set an IP precedence of 3 for routes matching prefix list 100.

```
<Sysname> system-view
[Sysname] ip prefix-list 100 permit 192.168.10.1 24
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match ip address prefix-list 100
[Sysname-route-policy-policy1-10] apply ip-precedence 3
```

apply preference

Use **apply preference** to set a preference for a routing protocol.

Use **undo apply preference** to restore the default.

Syntax

apply preference *preference*

undo apply preference

Default

No preference is set for a routing protocol.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

preference: Specifies a preference in the range of 1 to 255.

Usage guidelines

If you have set preferences for routing protocols by using the **preference** command, the **apply preference** command sets a new preference for the matching routing protocol. Unmatched routing protocols still use the preferences set by using the **preference** command.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to set the preference for OSPF external routes to 90.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match route-type external-type1or2
[Sysname-route-policy-policy1-10] apply preference 90
```

apply prefix-priority

Use **apply prefix-priority** to set a prefix priority for routes.

Use **undo apply prefix-priority** to restore the default.

Syntax

apply prefix-priority { **critical** | **high** | **medium** }

undo apply prefix-priority

Default

No prefix priority is set, which means the prefix priority is low.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

critical: Sets the critical prefix priority for routes.

high: Sets the high prefix priority for routes.

medium: Sets the medium prefix priority for routes.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to set prefix priority **critical** for routes matching prefix list **abc**.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match ip address prefix-list abc
[Sysname-route-policy-policy1-10] apply prefix-priority critical
```

apply tag

Use **apply tag** to set a tag for IGP routes.

Use **undo apply tag** to restore the default.

Syntax

apply tag *tag-value*

undo apply tag

Default

No routing tag is set for IGP routes.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

tag-value: Specifies the tag value in the range of 0 to 4294967295.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to set a tag of 100 for IGP routes.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] apply tag 100
```

continue

Use **continue** to specify the next node to be matched.

Use **undo continue** to restore the default.

Syntax

continue [*node-number*]

undo continue

Default

No next node is specified.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

node-number: Specifies the routing policy node number in the range of 0 to 65535.

Usage guidelines

The specified next node must have a larger number than the current node.

Example

Specify the next node 20 for node 10 of the routing policy **policy1**.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] continue 20
```

display route-policy

Use **display route-policy** to display routing policy information.

Syntax

display route-policy [**name** *route-policy-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters. If you do not specify this option, the command displays information about all routing policies.

Examples

Display information about routing policy **policy1**.

```
<Sysname> display route-policy name policy1
Route-policy: policy1
  Permit : 1
          if-match cost 10
          continue: next node 11
          apply preference 10
```

Table 1 Command output

Field	Description
Route-policy	Routing policy name.

permit	Match mode: • **Permit**. • **Deny**.
if-match	Match criterion.
continue	Specify the next node to be matched.
apply	Action.

if-match cost

Use **if-match cost** to match routes that have the specified cost.

Use **undo if-match cost** to restore the default.

Syntax

if-match cost *cost-value*

undo if-match cost

Default

No cost match criterion is configured.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

cost-value: Specifies a cost in the range of 0 to 4294967295.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to permit routes with a cost of 8.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match cost 8
```

if-match interface

Use **if-match interface** to match routes that have the specified output interfaces.

Use **undo if-match interface** to remove the specified output interface match criterion.

Syntax

if-match interface { *interface-type interface-number* }&<1-16>

undo if-match interface [*interface-type interface-number*]&<1-16>

Default

No output interface match criterion is configured.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

&<1-16>: Indicates that you can specify a maximum of 16 interfaces.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to permit routes with the output interface VLAN-interface 1.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match interface vlan-interface 1
```

if-match route-type

Use **if-match route-type** to set a route-type match criterion.

Use **undo if-match route-type** to remove the specified route-type match criterion.

Syntax

if-match route-type { **external-type1** | **external-type1or2** | **external-type2** | **internal** | **nssa-external-type1** | **nssa-external-type1or2** | **nssa-external-type2** } *

undo if-match route-type [**external-type1** | **external-type1or2** | **external-type2** | **internal** | **nssa-external-type1** | **nssa-external-type1or2** | **nssa-external-type2**] *

Default

No route-type match criterion is set.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

external-type1: Matches OSPF Type 1 external routes.

external-type1or2: Matches OSPF Type 1 and Type 2 external routes.

external-type2: Matches OSPF Type 2 external routes.

internal: Matches OSPF internal routes (including OSPF intra-area and inter-area routes).

nssa-external-type1: Matches OSPF NSSA Type 1 external routes.

nssa-external-type1or2: Matches OSPF NSSA Type 1 and 2 external routes.

nssa-external-type2: Matches OSPF NSSA Type 2 external routes.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to match OSPF internal routes.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
```

```
[Sysname-route-policy-policy1-10] if-match route-type internal
```

if-match tag

Use **if-match tag** to match IGP routes that have the specified tag.

Use **undo if-match tag** to restore the default.

Syntax

if-match tag *tag-value*

undo if-match tag

Default

No tag match criterion is configured.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

tag-value: Specifies a tag in the range of 0 to 4294967295.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to match IGP routes that have a tag of 8.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match tag 8
```

route-policy

Use **route-policy** to create a routing policy and a node and enter routing policy node view, or enter the view of an existing routing policy node.

Use **undo route-policy** to remove a routing policy or a node of it.

Syntax

route-policy *route-policy-name* { **deny** | **permit** } **node** *node-number*

undo route-policy *route-policy-name* [**deny** | **permit**] [**node** *node-number*]

Default

No routing policies exist.

Views

System view

Predefined user roles

network-admin

Parameters

route-policy-name: Specifies a routing policy name, a case-sensitive string of 1 to 63 characters.

deny: Specifies the deny match mode for the routing policy node. If a route matches all the **if-match** clauses of the node, it is denied without being compared with the next node. If a route does not match any **if-match** clauses of the node, the route is compared with the next node.

permit: Specifies the permit match mode for the routing policy node. If a route matches all the **if-match** clauses of the node, it is handled by the **apply** clauses of the node. If a route does not match any **if-match** clauses of the node, the route is compared with the next node.

node *node-number*: Specifies a node number in the range of 0 to 65535. A node with a smaller number is matched first.

Usage guidelines

Use a routing policy to filter routing information. A routing policy can contain several nodes and each node contains a set of **if-match** and **apply** clauses. The **if-match** clauses define the match criteria of the node and the **apply** clauses define the actions to be taken on packets matching the criteria. The relation between the **if-match** clauses of a node is logical AND. All the **if-match** clauses must be met. The relation between nodes is logical OR. A packet passing a node passes the routing policy. If a packet does not pass any nodes, the packet does not pass the routing policy.

Examples

Create node 10 in **permit** mode for routing policy **policy1** and enter routing policy node view.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10]
```

Related commands

display route-policy

route-policy-change delay-time

Use **route-policy-change delay-time** to set the routing policy change delay timer.

Use **undo route-policy-change delay-time** to restore the default.

Syntax

route-policy-change delay-time { *time-value* | **unlimited** }

undo route-policy-change delay-time

Default

Routing policy changes immediately take effect, but the routing protocol waits five seconds before processing routes from the new routing policy.

Views

System view

Predefined user roles

network-admin

Parameters

time-value: Specifies the routing policy change delay timer in the range of 60 to 3600 seconds. When this delay timer expires, the routing protocol waits five seconds before processing routes from the new routing policy.

unlimited: Sets an infinite delay timer.

Usage guidelines

This command makes a routing policy take effect after a delayed time interval, which prevents incomplete routing policy configuration from being issued to cause incorrect route advertisement. The system automatically starts the timer when a routing policy changes. The changes will not take effect on the routing policy until the change delay timer expires.

A routing policy changes when one of the following events occurs:

- A routing policy is created.
- A routing policy node, **if-match** clause, or **apply** clause is added, modified, or deleted for a routing policy.
- An IPv4 prefix list, IPv6 prefix list, AS path list, community list, extended community list, or MAC list is added, modified, or deleted.
- The ACL used by an **if-match** clause changes.

To have enough time to complete routing policy configuration, you can specify the **unlimited** keyword for the command. Then, execute the **undo** form of the command after you complete the configuration.

If you modify the routing policy change delay timer before it expires, the timer will be reset.

Examples

Set the routing policy change delay timer to 60 seconds.

```
<Sysname> system-view
[Sysname] route-policy-change delay-time 6
```

IPv4 routing policy commands

apply fast-reroute

Use **apply fast-reroute** to set a backup link for fast reroute (FRR).

Use **undo apply fast-reroute** to restore the default.

Syntax

apply fast-reroute { **backup-interface** *interface-type interface-number* [**backup-nexthop** *ip-address*] | **backup-nexthop** *ip-address* }

undo apply fast-reroute

Default

No backup link for FRR is configured.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

backup-interface *interface-type interface-number*: Specifies a backup output interface by its type and number. If the specified interface is a non-P2P interface, you must also specify a backup next hop. Non-P2P interfaces include NBMA and broadcast interfaces.

backup-nexthop *ip-address*: Specifies a backup next hop.

Examples

Configure node 10 of routing policy **policy1** to set the backup output interface VLAN-interface 1 and backup next hop 193.1.1.8 for the route destined for 100.1.1.0/24.

```
<Sysname> system-view
[Sysname] ip prefix-list abc index 10 permit 100.1.1.0 24
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match ip address prefix-list abc
[Sysname-route-policy-policy1-10] apply fast-reroute backup-interface vlan-interface 1
backup-nexthop 193.1.1.8
```

apply ip-address next-hop

Use **apply ip-address next-hop** to set a next hop for IPv4 routes.

Use **undo apply ip-address next-hop** to restore the default.

Syntax

apply ip-address next-hop *ip-address* [**public**]

undo apply ip-address next-hop

Default

No next hop is set for IPv4 routes.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the next hop IP address.

public: Specifies the public network.

Usage guidelines

If you use this command to set a next hop for redistributed routes, the configuration does not take effect.

If you do not specify the **public** keyword, the next hop belongs to the public network.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to set next hop 193.1.1.8 for routes matching prefix list 100.

```
<Sysname> system-view
[Sysname] ip prefix-list 100 permit 192.168.10.1 24
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match ip address prefix-list 100
[Sysname-route-policy-policy1-10] apply ip-address next-hop 193.1.1.8
```

display ip prefix-list

Use **display ip prefix-list** to display IPv4 prefix list statistics.

Syntax

display ip prefix-list [**name** *prefix-list-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *prefix-list-name*: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters. If you do not specify this option, the command displays statistics for all IPv4 prefix lists.

Examples

Display the statistics for IPv4 prefix list **abc**.

```
<Sysname> display ip prefix-list name abc
Prefix-list: abc
 Permitted 0
 Denied 0
        index: 10        Deny   6.6.6.0/24              ge  26  le  28
```

Table 2 Command output

Field	Description
Prefix-list	Name of the IPv4 prefix list.
Permitted	Number of routes matching the criterion.
Denied	Number of routes not matching the criterion.
index	Index of an item.
deny	Match mode of the item: • **Permit**. • **Deny**.
6.6.6.0/24	IP address and mask.
ge	Greater-equal, the lower mask length limit.
le	Less-equal, the upper mask length limit.

Related commands

ip prefix-list

reset ip prefix-list

if-match ip

Use **if-match ip** to match IPv4 routes whose destination, next hop, or source address matches an ACL or IPv4 prefix list.

Use **undo if-match ip** to remove the specified ACL or IPv4 prefix list match criterion.

Syntax

if-match ip { **address** | **next-hop** } { **acl** *ipv4-acl-number* | **prefix-list** *prefix-list-name* }

undo if-match ip { **address** | **next-hop** | **route-source** } [**acl** | **prefix-list**]

Default

No ACL or IPv4 prefix list match criterion is configured.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

address: Matches the destination address of IPv4 routes.

next-hop: Matches the next hop of IPv4 routes.

acl *ipv4-acl-number*: Specifies an ACL by its number. The value range for the *ipv4-acl-number* argument is 2000 to 3999 for the **address** keyword, and 2000 to 2999 for the **next-hop** keyword and **route-source** keyword.

prefix-list *prefix-list-name*: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters.

Examples

Configure node 10 of routing policy **policy1** to match IPv4 routes whose next hop matches IP prefix list **p1**.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match ip next-hop prefix-list p1
```

ip prefix-list

Use **ip prefix-list** to configure an IPv4 prefix list or an item for the list.

Use **undo ip prefix-list** to remove an IPv4 prefix list or an item of it.

Syntax

ip prefix-list *prefix-list-name* [**index** *index-number*] { **deny** | **permit** } *ip-address mask-length* [**greater-equal** *min-mask-length*] [**less-equal** *max-mask-length*]

undo ip prefix-list *prefix-list-name* [**index** *index-number*]

Default

No IPv4 prefix lists exist.

Views

System view

Predefined user roles

network-admin

Parameters

prefix-list-name: Specifies an IPv4 prefix list name, a case-sensitive string of 1 to 63 characters.

index *index-number*: Specifies an index number for an IPv4 prefix list item, in the range of 1 to 65535. An item with a smaller index number is matched first. If you do not specify this option, the index number starts from 10 and increments by 10 for each of the consecutive prefix list items.

deny: Specifies the deny mode. If a route matches the item, the route is denied without being compared with the next item. If a route does not match the item, the route is compared with the next item.

permit: Specifies the permit mode. If a route matches the item, it passes the IPv4 prefix list. If a route does not match the item, the route is compared with the next item.

ip-address mask-length: Specifies an IPv4 prefix and mask length. The value range for the *mask-length* argument is 0 to 32.

greater-equal *min-mask-length*, **less-equal** *max-mask-length*: Specifies a prefix length range. The **greater-equal** keyword means "greater than or equal to" and the **less-equal** keyword means "less than or equal to." The prefix length range relation is *mask-length* <= *min-mask-length* <= *max-mask-length* <= 32.

- If only the *min-mask-length* argument is specified, the prefix length range is [*min-mask-length*, 32].
- If only the *max-mask-length* argument is specified, the prefix length range is [*mask-length*, *max-mask-length*].
- If both the *min-mask-length* and *max-mask-length* arguments are specified, the prefix length range is [*min-mask-length*, *max-mask-length*].

Usage guidelines

An IPv4 prefix list is used to filter IPv4 addresses. It can contain multiple items, each of which specifies a range of IPv4 prefixes. The relation between the items is logical OR. If an item is passed, the IPv4 prefix list is passed. If no item is passed, the IP prefix list cannot be passed.

If both the *ip-address* and *mask-length* arguments are specified as 0.0.0.0 0, only the default route will be matched.

To match all routes, use 0.0.0.0 0 **less-equal** 32.

Examples

Configure IP prefix list **p1** to permit routes destined for network 10.0.0.0/8 and with mask length 17 or 18.

```
<Sysname> system-view
[Sysname] ip prefix-list p1 permit 10.0.0.0 8 greater-equal 17 less-equal 18
```

Related commands

display ip prefix-list

reset ip prefix-list

reset ip prefix-list

Use **reset ip prefix-list** to clear IPv4 prefix list statistics.

Syntax

reset ip prefix-list [*prefix-list-name*]

Views

User view

Predefined user roles

network-admin

Parameters

prefix-list-name: Specifies an IP prefix list by its name, a case-sensitive string of 1 to 63 characters. If you do not specify this argument, the command clears statistics for all IPv4 prefix lists.

Examples

Clear the statistics for IPv4 prefix list **abc**.

```
<Sysname> reset ip prefix-list abc
```

Related commands

display ip prefix-list

ip prefix-list

IPv6 routing policy commands

apply ipv6 fast-reroute

Use **apply ipv6 fast-reroute** to set a backup link for fast reroute (FRR).

Use **undo apply ipv6 fast-reroute** to restore the default.

Syntax

apply ipv6 fast-reroute { **backup-interface** *interface-type interface-number* [**backup-nexthop** *ipv6-address*] | **backup-nexthop** *ipv6-address* }

undo apply ipv6 fast-reroute

Default

No backup link for FRR is configured.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

backup-interface *interface-type interface-number*: Specifies a backup output interface by its type and number. If the specified interface is a non-P2P interface, you must also specify a backup next hop. Non-P2P interfaces include NBMA and broadcast interfaces.

backup-nexthop *ipv6-address*: Specifies an IPv6 backup next hop.

Examples

Configure node 10 of routing policy **policy1** to set the backup next hop 1::1/64 for the route destined for 100::1/64.

```
<Sysname> system-view
[Sysname] ipv6 prefix-list abc index 10 permit 100::1 64
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match ipv6 address prefix-list abc
[Sysname-route-policy-policy1-10] apply ipv6 fast-reroute backup-nexthop 1::1
```

apply ipv6 next-hop

Use **apply ipv6 next-hop** to set a next hop for IPv6 routes.

Use **undo apply ipv6 next-hop** to restore the default.

Syntax

apply ipv6 next-hop *ipv6-address*

undo apply ipv6 next-hop

Default

No next hop is set for IPv6 routes.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the next hop IPv6 address.

Usage guidelines

If you use this command to set a next hop for redistributed routes, the configuration does not take effect.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to set next hop 3ffe:506::1 for IPv6 routes matching prefix list 100.

```
<Sysname> system-view
[Sysname] ipv6 prefix-list 100 permit 2::2 64
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match ipv6 address prefix-list 100
[Sysname-route-policy-policy1-10] apply ipv6 next-hop 3ffe:506::1
```

display ipv6 prefix-list

Use **display ipv6 prefix-list** to display IPv6 prefix list statistics.

Syntax

display ipv6 prefix-list [**name** *prefix-list-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *prefix-list-name*: Specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters. If you do not specify this option, the command displays statistics for all IPv6 prefix lists.

Examples

Display the statistics for all IPv6 prefix lists.

```
<Sysname> display ipv6 prefix-list
Prefix-list6: 666
 Permitted 0
 Denied 0
        index: 10        Permit 6::/64                 ge  66  le  88
```

Table 3 Command output

Field	Description
Prefix-list6	Name of the IPv6 prefix list.
Permitted	Number of routes matching the criterion.
Denied	Number of routes not matching the criterion.
index	Index number of an item.
permit	Match mode of the item: • **Permit**. • **Deny**.
6::/64	IPv6 address and prefix length for matching.
ge	Greater-equal, the lower prefix length limit.
le	Less-equal, the upper prefix length limit.

Related commands

ipv6 prefix-list

reset ipv6 prefix-list

if-match ipv6

Use **if-match ipv6** to match IPv6 routes whose destination, next hop, or source address matches an ACL or IPv6 prefix list.

Use **undo if-match ipv6** to remove the specified ACL or IPv6 prefix list match criterion.

Syntax

if-match ipv6 { **address** | **next-hop** | **route-source** } { **acl** *ipv6-acl-number* | **prefix-list** *prefix-list-name*

undo if-match ipv6 { **address** | **next-hop** | **route-source** } [**acl** | **prefix-list**]

Default

No ACL or IPv6 prefix list match criterion is configured.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

address: Matches the destination address of IPv6 routes.

next-hop: Matches the next hop of IPv6 routes.

route-source: Matches the source address of IPv6 routes.

acl *ipv6-acl-number*: Specifies an IPv6 ACL by its number. The value range for the *ipv6-acl-number* argument is 2000 to 3999 for the **address** keyword, and 2000 to 2999 for the **next-hop** and **route-source** keywords.

prefix-list *prefix-list-name*: Specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters.

Examples

Configure node 10 of routing policy **policy1** to permit routes whose next hop matches IPv6 prefix list **p1**.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match ipv6 next-hop prefix-list p1
```

ipv6 prefix-list

Use **ipv6 prefix-list** to configure an IPv6 prefix list or an item for it.

Use **undo ipv6 prefix-list** to remove an IPv6 prefix list or an item.

Syntax

ipv6 prefix-list *prefix-list-name* [**index** *index-number*] { **deny** | **permit** } *ipv6-address* { *prefix-length* [**greater-equal** *min-prefix-length*] [**less-equal** *max-prefix-length*] | **inverse** *inverse-prefix-length* }

undo ipv6 prefix-list *prefix-list-name* [**index** *index-number*]

Default

No IPv6 prefix lists exist.

Views

System view

Predefined user roles

network-admin

Parameters

prefix-list-name: Specifies an IPv6 prefix list name, a case-sensitive string of 1 to 63 characters.

index *index-number*: Specifies an index number for an IPv6 prefix list item, in the range of 1 to 65535. An item with a smaller index number is matched first. If you do not specify this option, the index number starts from 10 and increments by 10 for each of the consecutive IPv6 prefix list items.

deny: Specifies the deny mode. If a route matches the item, the route is denied without being compared with the next item. If a route does not match the item, the route is compared with the next item.

permit: Specifies the permit mode. If a route matches the item, it passes the IPv6 prefix list. If a route does not match the item, the route is compared with the next item.

ipv6-address: Specifies an IPv6 address.

prefix-length: Specifies the IPv6 prefix length. The value range for the *prefix-length* argument is 0 to 128.

greater-equal *min-mask-length*, **less-equal** *max-mask-length*: Specifies a prefix length range. The **greater-equal** keyword means "greater than or equal to" and the **less-equal** keyword means "less than or equal to."

The prefix length range relation is *mask-length* <= *min-mask-length* <= *max-mask-length* <= 128.

- If only the *min-prefix-length* argument is specified, the prefix length range is [*min-prefix-length*, 128].
- If only the *max-prefix-length* argument is specified, the prefix length range is [*prefix-length*, *max-prefix-length*].
- If both the *min-prefix-length* and *max-prefix-length* arguments are specified, the prefix length range is [*min-prefix-length*, *max-prefix-length*].

inverse *inverse-prefix-length*: Matches IPv6 addresses from the least significant bit to the specified length. The value range for the *inverse-prefix-length* argument is 1 to 128.

Usage guidelines

An IPv6 prefix list is used to filter IPv6 addresses. An IPv6 prefix list can have multiple items, and each of them specifies a range of IPv6 prefixes. The relation between the items is logical OR. A route passing an item passes the IPv6 prefix list. A route passing no item does not pass the IPv6 prefix list.

If the *ipv6-address prefix-length* argument is specified as :: 0, only the default route matches.

To match all routes, configure :: 0 **less-equal** 128.

Examples

Permit IPv6 addresses with a mask length between 32 bits and 64 bits.

```
<Sysname> system-view
[Sysname] ipv6 prefix-list abc permit :: 0 greater-equal 32 less-equal 64
```

Deny IPv6 addresses with a prefix 3FFE:D00::/32 and a prefix length greater than or equal to 32 bits.

```
<Sysname> system-view
[Sysname] ipv6 prefix-list abc deny 3FFE:D00:: 32 less-equal 128
```

Related commands

display ipv6 prefix-list

reset ipv6 prefix-list

reset ipv6 prefix-list

Use **reset ipv6 prefix-list** to clear IPv6 prefix list statistics.

Syntax

reset ipv6 prefix-list [*prefix-list-name*]

Views

User view

Predefined user roles

network-admin

Parameters

prefix-list-name: Specifies an IPv6 prefix list by its name, a case-sensitive string of 1 to 63 characters. If you do not specify this argument, the command clears statistics for all IPv6 prefix lists.

Examples

Clear the statistics for IPv6 prefix list **abc**.

```
<Sysname> reset ipv6 prefix-list abc
```

Related commands

display ipv6 prefix-list

ipv6 prefix-list

IP Multicast Command Reference

This command reference is applicable to the following switches and software versions:

H3C S5120V2-LI switch series (Release 6308P01 and later)
H3C S3100V3-SI switch series (Release 6309P01 and later)
H3C S5110V2 switch series (Release 6310 and later)
H3C S5110V2-SI switch series (Release 6310 and later)
H3C S5000V3-EI switch series (Release 6310 and later)
H3C S5000V5-EI switch series (Release 6319P01 and later)
H3C S5000E-X switch series (Release 6310 and later)
H3C S5130S-LI switch series (Release 6310 and later)
H3C MS4320V2 switch series (Release 6308P01 and later)
H3C MS4320 switch series (Release 6308P01 and later)
H3C MS4300V2 switch series (Release 6308P01 and later)
H3C MS4200 switch series (Release 6310 and later)
H3C WS5810-WiNet switch series (Release 6308P01 and later)
H3C WS5820-WiNet switch series (Release 6308P01 and later)
H3C WAS6000 switch series (Release 6308P01 and later)
H3C S5000X-EI switch series (Release 6329 and later)
H3C MS4320V3 switch series (Release 6329 and later)
H3C S5120V3-SI switch series (Release 6329 and later)
H3C S5120V3-LI switch series (Release 6329 and later)

New H3C Technologies Co., Ltd.
http://www.h3c.com

Software version: Release 63xx
Document version: 6W105-20230524

Preface

This command reference describes IP multicast configuration commands. It covers the commands for configuring IPv4 multicast and IPv6 multicast. With these multicast configuration commands, you can implement efficient point-to-multipoint data transmission in your network.

This preface includes the following topics about the documentation:

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** >

Convention	Description
	Folder.

Symbols

Convention	Description
⚠ **WARNING!**	An alert that calls attention to important information that if not understood or followed can result in personal injury.
△ **CAUTION:**	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
ⓘ **IMPORTANT:**	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Documentation feedback

You can e-mail your comments about product documentation to info@h3c.com.

We appreciate your comments.

Contents

IGMP snooping commands

display igmp-snooping

Use **display igmp-snooping** to display IGMP snooping status.

Syntax

display igmp-snooping [**global** | **vlan** *vlan-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

global: Displays the global IGMP snooping status.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

Usage guidelines

If you do not specify any parameters, this command displays the global IGMP snooping status and the IGMP snooping status in all VLANs.

Examples

Display the global IGMP snooping status and the IGMP snooping status for all VLANs.

```
<Sysname> display igmp-snooping
IGMP snooping information: Global
 Global-enable: Enabled
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-member-query-interval: 1s
 Report-aggregation: Enabled
 Host-tracking: Disabled
 Dot1p-priority: --

IGMP snooping information: VLAN 1
 IGMP snooping: Enabled
 Drop-unknown: Disabled
 Version: 2
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-member-query-interval: 1s
 Querier: Enabled (IP: 1.1.1.1, Expires: 00:02:05)
 Querier-election: Enabled
 Query-interval: 125s
 General-query source IP: 1.1.1.1
```

```
 Special-query source IP: 2.2.2.2
 Report source IP: 3.0.0.3
 Leave source IP: 1.0.0.1
 Host-tracking: Disabled
 Dot1p-priority: 2
 Proxy: Disabled

IGMP snooping information: VLAN 10
 IGMP snooping: Enabled
 Drop-unknown: Enabled
 Version: 3
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-member-query-interval: 1s
 Querier: Enabled (IP: 1.1.1.1, Expires: 00:02:05)
 Querier-election: Enabled
 Query-interval: 125s
 General-query source IP: 1.1.1.1
 Special-query source IP: 2.2.2.2
 Report source IP: 3.0.0.3
 Leave source IP: 1.0.0.1
 Host-tracking: Disabled
 Dot1p-priority: --
 Proxy: Disabled
```

Table 1 Command output

Field	Description
Global-enable	Global IGMP snooping status: • Enabled. • Disabled.
IGMP snooping	IGMP snooping status in a VLAN: • **Enabled**. • **Disabled**. • **Globally enabled**. • **Inactive**—IGMP snooping configuration does not take effect.
Drop-unknown	Status of dropping unknown multicast data: • Enabled. • Disabled.
Version	IGMP snooping version.
Host-aging-time	Aging timer for the dynamic member port.
Router-aging-time	Aging timer for the dynamic router port.
Max-response-time	Maximum response time for IGMP general queries.
Last-member-query-interval	Interval for sending IGMP group-specific queries.
Report-aggregation	Status of IGMP report suppression: • Enabled.

Field	Description
	• Disabled.
Dot1p-priority	802.1p priority for IGMP messages. If the priority is not configured, this field displays two hyphens (--).
Querier	Status of IGMP snooping querier: • Enabled. • Disabled.
(IP: 1.1.1.1, Expires: 00:02:05)	IGMP snooping querier information: • **IP**—IP address of the IGMP snooping querier. • **Expire**—Remaining aging time for the IGMP snooping querier. This field is not displayed if IGMP snooping querier election is disabled.
Querier-election	Status of IGMP snooping querier election: • Enabled. • Disabled.
Query-interval	Interval for sending IGMP general queries.
General-query source IP	Source IP address of IGMP general queries.
Special-query source IP	Source IP address of IGMP group-specific queries.
Report source IP	Source IP address of IGMP reports.
Leave source IP	Source IP address of IGMP leave messages.
Host-tracking	Status of host tracking: • Enabled • Disabled. • Globally enabled.
Proxy	Status of IGMP snooping proxying: • Enabled. • Disabled.

display igmp-snooping group

Use **display igmp-snooping group** to display information about dynamic IGMP snooping group entries.

Syntax

display igmp-snooping group [*group-address* | *source-address*] * [**vlan** *vlan-id*] [**interface** *interface-type interface-number* | [**verbose**] [**slot** *slot-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group-address: Specifies a multicast group by its IP address in the range of 224.0.1.0 to 239.255.255.255. If you do not specify a multicast group, this command displays information about dynamic IGMP snooping group entries for all multicast groups.

source-address: Specifies a multicast source by its IP address. If you do not specify a multicast source, this command displays information about dynamic IGMP snooping group entries for all multicast sources.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays information about dynamic IGMP snooping group entries for all VLANs.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays brief information about dynamic IGMP snooping group entries for all interfaces.

verbose: Displays detailed information about dynamic IGMP snooping group entries. If you do not specify this keyword, the command displays brief information about dynamic IGMP snooping group entries.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about dynamic IGMP snooping group entries for the master device.

Examples

Display brief information about dynamic IGMP snooping group entries for GigabitEthernet 1/0/1.

```
<Sysname> display igmp-snooping group interface gigabitethernet 1/0/1
Total 1 entries.

GE1/0/1:
  VLAN 2: Total 1 entries.
   (0.0.0.0, 224.1.1.1)                    (00:03:23)
```

Display detailed information about dynamic IGMP snooping group entries for VLAN 2.

```
<Sysname> display igmp-snooping group vlan 2 verbose
Total 2 entries.

VLAN 2: Total 2 entries.
  (0.0.0.0, 224.1.1.1)
    Attribute: local port
    FSM information: dummy
    Host slots (0 in total):
    Host ports (1 in total):
      GE1/0/2                               (00:03:23)
  (1.1.1.1, 224.1.1.1)
    Attribute: local port
    FSM information: dummy
    Host ports (1 in total):
      GE1/0/2                               (00:04:04)
```

Table 2 Command output

Field	Description
Total 1 entries	Total number of dynamic IGMP snooping group entries.

Field	Description
VLAN 2: Total 1 entries	Total number of dynamic IGMP snooping group entries in VLAN 2.
(0.0.0.0, 224.1.1.1)	(S, G) entry, where **0.0.0.0** in the S position means all multicast sources.
Attribute	Entry attribute: • **global port**—The entry has a global port. • **local port**—The entry has a port that resides on the member device for which the information is displayed. • **slot**—The entry has ports that reside on other member devices except the member device for which the information is displayed.
FSM information	Finite state machine information of the entry: • **delete**—The entry attributes have been deleted. • **dummy**—The entry is a new temporary entry. • **no info**—No entry exists. • **normal**—The entry is a correct entry.
Host slots (0 in total)	Member IDs and total number of the member devices that have member ports, except for the specified member device or the master device when no member device is specified.
Host ports (1 in total)	Member ports, and the total number of member ports.
(00:03:23)	Remaining aging time for the dynamic member port. For a global port (such as Layer 2 aggregate interfaces), this field is always displayed. For a non-global port, this field is displayed when one of the following conditions exists: • The port is on the specified member device. • The port is on the master device and no member device is specified.

Related commands

`reset igmp-snooping group`

display igmp-snooping host-tracking

Use **`display igmp-snooping host-tracking`** to display host tracking information.

Syntax

`display igmp-snooping host-tracking vlan` *`vlan-id`* **`group`** *`group-address`* [**`source`** *`source-address`*] [**`slot`** *`slot-number`*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

`vlan` *`vlan-id`*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

`group` *`group-address`*: Specifies a multicast group by its IP address in the range of 224.0.1.0 to 239.255.255.255.

source *source-address*: Specifies a multicast source by its IP address. If you do not specify a multicast source, this command displays host tracking information for all multicast sources.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays host tracking information for the master device.

Examples

Display tracking information for hosts that have joined multicast group 224.1.1.1 in VLAN 2.

```
<Sysname> display igmp-snooping host-tracking vlan 2 group 224.1.1.1
VLAN 2
  (0.0.0.0, 224.1.1.1)
    Port: GE1/0/1
      Host                                    Uptime          Expires
      1.1.1.1                                 00:02:20        00:00:40
      2.2.2.2                                 00:02:21        00:00:39
```

Table 3 Command output

Field	Description
VLAN	VLAN ID.
(0.0.0.0, 224.1.1.1)	(S, G) entry, where 0.0.0.0 in the S position means any multicast sources.
Port	Member port.
Host	IP address of the host.
Uptime	Length of time elapsed since the host joined the multicast group.
Expires	Remaining timeout time for the host. The host timeout time is the same as the aging timer for the port. The timer is reset when the port receives an IGMP report from the host. This field displays **timeout** if the host times out.

Related commands

host-tracking (IGMP-snooping view)

igmp-snooping enable

igmp-snooping host-tracking

display igmp-snooping router-port

Use **display igmp-snooping router-port** to display dynamic router port information.

Syntax

display igmp-snooping router-port [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

verbose: Displays detailed information. If you do not specify the keyword, this command displays brief information.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays dynamic router port information for all VLANs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays dynamic router port information for the master device.

Examples

Display brief information about dynamic router ports for VLAN 2.

```
<Sysname> display igmp-snooping router-port vlan 2
VLAN 2:
  Router ports (2 in total):
    GE1/0/1                                (00:01:30)
    GE1/0/2                                (00:00:23)
```

Display detailed information about dynamic router ports for VLAN 2.

```
<Sysname> display igmp-snooping router-port vlan 2 verbose
VLAN 2:
  Router slots (0 in total):
  Router ports (2 in total):
    GE1/0/1                              (00:01:30)
    GE1/0/2                              (00:00:23)
```

Table 4 Command output

Field	Description
VLAN 2	VLAN ID.
Router slots (0 in total)	Member IDs and total number of the member devices that have dynamic router ports, except for the specified member device or the master device when no member device is specified.
Router ports (2 in total)	Dynamic router ports and total number of dynamic router ports.
(00:01:30)	Remaining aging time for the dynamic router port. For a global port, this field is always displayed. For a global port, this field is displayed when one of the following conditions exists: • The port is on the specified member device. • The port is on the master device and no member device is specified.

Related commands

reset igmp-snooping router-port

display igmp-snooping static-group

Use **display igmp-snooping static-group** to display information about static IGMP snooping group entries.

Syntax

display igmp-snooping static-group [*group-address* | *source-address*] * [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group-address: Specifies a multicast group by its IP address in the range of 224.0.1.0 to 239.255.255.255. If you do not specify a multicast group, this command displays information about static IGMP snooping group entries for all multicast groups.

source-address: Specifies a multicast source by its IP address. If you do not specify a multicast source, this command displays information about static IGMP snooping group entries for all multicast sources.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays information about static IGMP snooping group entries for all VLANs.

verbose: Displays detailed information about static IGMP snooping group entries. If you do not specify the keyword, this command displays brief information about static IGMP snooping group entries.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about static IGMP snooping group entries for the master device.

Examples

Display detailed information about static IGMP snooping group entries for VLAN 2.

```
<Sysname> display igmp-snooping static-group vlan 2 verbose
Total 1 entries.

VLAN 2: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Attribute: local port
    FSM information: dummy
    Host slots (0 in total):
    Host ports (1 in total):
      GE1/0/2
```

Table 5 Command output

Field	Description
Total 1 entries	Total number of static IGMP snooping group entries.
VLAN 2: Total 1 entries	Total number of static IGMP snooping group entries in VLAN 2.
(0.0.0.0, 224.1.1.1)	(S, G) entry, where **0.0.0.0** in the S position means all multicast sources.
Attribute	Entry attribute: • **global port**—The entry has a global port. • **local port**—The entry has a port that resides on the member device for which the information is displayed. • **slot**—The entry has ports that reside on other member devices except the member device for which the information is displayed.
FSM information	Finite state machine information of the entry: • **delete**—The entry attributes have been deleted.

Field	Description
	• **dummy**—The entry is a new temporary entry. • **no info**—No entry exists. • **normal**—The entry is a correct entry.
Host slots (0 in total)	Member IDs and total number of the member devices that have member ports, except for the specified member device or the master device when no member device is specified.
Host ports (1 in total)	Member ports and total number of member ports.

display igmp-snooping static-router-port

Use **display igmp-snooping static-router-port** to display static router port information.

Syntax

display igmp-snooping static-router-port [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

verbose: Displays detailed information about static router ports. If you do not specify this keyword, the command displays brief information about static router ports.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays static router port information for the master device.

Examples

Display brief information about static router ports for VLAN 2.

```
<Sysname> display igmp-snooping static-router-port vlan 2
VLAN 2:
  Router ports (2 in total):
    GE1/0/1
    GE1/0/2
```

Display detailed information about static router ports for VLAN 2.

```
<Sysname> display igmp-snooping static-router-port vlan 2 verbose
VLAN 2:
  Router slots (0 in total):
  Router ports (2 in total):
    GE1/0/1
    GE1/0/2
```

Table 6 Command output

Field	Description
VLAN 2	VLAN ID.
Router slots (0 in total)	Member IDs and total number of the member devices that have static router ports, except for the specified member device or the master device when no member device is specified.
Router ports (2 in total)	Static router ports and total number of static router ports.

display igmp-snooping statistics

Use **display igmp-snooping statistics** to display statistics for the IGMP messages and PIMv2 hello messages learned through IGMP snooping.

Syntax

display igmp-snooping statistics

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display statistics for the IGMP messages and PIMv2 hello messages learned through IGMP snooping.

```
<Sysname> display igmp-snooping statistics
Received IGMP general queries:  0
Received IGMPv1 reports:  0
Received IGMPv2 reports:  19
Received IGMP leaves:  0
Received IGMPv2 specific queries:  0
Sent     IGMPv2 specific queries:  0
Received IGMPv3 reports:  1
Received IGMPv3 reports with right and wrong records:  0
Received IGMPv3 specific queries:  0
Received IGMPv3 specific sg queries:  0
Sent     IGMPv3 specific queries:  0
Sent     IGMPv3 specific sg queries:  0
Received PIMv2 hello:  0
Received error IGMP messages:  19
```

Table 7 Command output

Field	Description
general queries	Number of IGMP general queries.
specific queries	Number of IGMP group-specific queries.
reports	Number of IGMP reports.

Field	Description
leaves	Number of IGMP leave messages.
reports with right and wrong records	Number of IGMP reports with correct and incorrect records.
specific sg queries	Number of IGMP group-and-source-specific queries.
PIMv2 hello	Number of PIMv2 hello messages.
error IGMP messages	Number of IGMP messages with errors.

Related commands

reset igmp-snooping statistics

display l2-multicast fast-forwarding cache

Use **display l2-multicast fast-forwarding cache** to display Layer 2 multicast fast forwarding entries.

Syntax

display l2-multicast fast-forwarding cache [**vlan** *vlan-id*] [*source-address* | *group-address*] * [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

source-address: Specifies a multicast source address. If you do not specify a multicast source, this command displays Layer 2 multicast fast forwarding entries for all multicast sources.

group-address: Specifies a multicast group address in the range of 224.0.1.0 to 239.255.255.255. If you do not specify a multicast group, this command displays Layer 2 multicast fast forwarding entries for all multicast groups.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays Layer 2 multicast fast forwarding entries for the master device.

Examples

Display Layer 2 multicast fast forwarding entries.

```
<Sysname> display l2-multicast fast-forwarding cache
Total 1 entries, 1 matched

(10.1.1.2,225.1.1.1)
     Status      : Enable                VLAN            : 1
     Source port : 9876                  Destination port: 5432
     Protocol    : 17                    Flag            : 0x2
     Ingress port: GigabitEthernet1/0/2
     List of 1 egress ports:
```

```
        GigabitEthernet1/0/3
        Status: Enable                Flag: 0x10
```

Table 8 Command output

Field	Description
Total 1 entries, 1 matched	Total number of (S, G) entries in the Layer 2 multicast fast forwarding table, and the total number of matching entries.
(10.1.1.2, 225.1.1.1)	(S, G) entry in the Layer 2 multicast fast forwarding table.
Protocol	Protocol number.
VLAN	VLAN ID.
Flag	Flag for the (S, G) entry or the outgoing port. This field displays one flag or the sum of multiple flags. In this example, the value 0x2 means that the entry has only one flag 0x2. The following flags are available for an entry: • **0x1**—The entry is created because of packets passed through between cards. • **0x2**—The entry is added by multicast forwarding. The following flags are available for an outgoing interface: • **0x1**—The port is added to the entry because of packets passed through between cards. • **0x2**—The port is added to an existing entry. • **0x10**—The port is associated with the entry. • **0x20**—The port is to be deleted.
Status	Status of the (S, G) entry or the outgoing port: • **Enabled**—Available. • **Disabled**—Unavailable.
Ingress port	Incoming port of the (S, G) entry.
List of 1 egress ports	Outgoing port list of the (S, G) entry.

Related commands

`reset l2-multicast fast-forwarding cache all`

display l2-multicast ip

Use **`display l2-multicast ip`** to display information about Layer 2 IP multicast groups.

Syntax

`display l2-multicast ip` [**`group`** *`group-address`* | **`source`** *`source-address`*] * [**`vlan`** *`vlan-id`*] [**`slot`** *`slot-number`*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group *group-address*: Specifies a multicast group by its IP address. If you do not specify a multicast group, this command displays information about all Layer 2 IP multicast groups.

source *source-address*: Specifies a multicast source by its IP address. If you do not specify a multicast source, this command displays information about Layer 2 IP multicast groups for all multicast sources.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays information about Layer 2 IP multicast groups for all VLANs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about Layer 2 IP multicast groups for the master device.

Examples

Display information about Layer 2 IP multicast groups for VLAN 2.

```
<Sysname> display l2-multicast ip vlan 2
Total 1 entries.

VLAN 2: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Attribute: static, success
    Host ports (1 in total):
      GE1/0/1                                (S, SUC)
```

Table 9 Command output

Field	Description
Total 1 entries	Total number of Layer 2 IP multicast groups.
VLAN 2: Total 1 entries	Total number of Layer 2 IP multicast groups in VLAN 2.
(0.0.0.0, 224.1.1.1)	(S, G) entry, where **0.0.0.0** in the S position means all multicast sources.
Attribute	Entry attribute: • **dynamic**—The entry is created by a dynamic protocol. • **static**—The entry is created by a static protocol. • **pim**—The entry is created by PIM. • **kernel**—The entry is obtained from the kernel. • **success**—Processing has succeeded. • **fail**—Processing has failed.
Host ports (1 in total)	Member ports and total number of member ports.
(S, SUC)	Port attribute: • **D**—Dynamic port. • **S**—Static port. • **P**—PIM port. • **K**—Port obtained from the kernel. • **R**—Port learned from (*, *) entries. • **W**—Port learned from (*, G) entries. • **SUC**—Processing has succeeded. • **F**—Processing has failed.

display l2-multicast ip forwarding

Use **display l2-multicast ip forwarding** to display Layer 2 multicast IP forwarding entries.

Syntax

display l2-multicast ip forwarding [**group** *group-address* | **source** *source-address*] * [**vlan** *vlan-id*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group *group-address*: Specifies a multicast group by its IP address. If you do not specify a multicast group, this command displays Layer 2 multicast IP forwarding entries for all multicast groups.

source *source-address*: Specifies a multicast source by its IP address. If you do not specify a multicast source, this command displays Layer 2 multicast IP forwarding entries for all multicast sources.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays Layer 2 multicast IP forwarding entries for all VLANs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays Layer 2 multicast IP forwarding entries for the master device.

Examples

Display Layer 2 multicast IP forwarding entries for VLAN 2.

```
<Sysname> display l2-multicast ip forwarding vlan 2
Total 1 entries.

VLAN 2: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Host ports (3 in total):
      GigabitEthernet1/0/1
      GigabitEthernet1/0/2
      GigabitEthernet1/0/3
```

Table 10 Command output

Field	Description
Total 1 entries	Total number of Layer 2 multicast IP forwarding entries.
VLAN 2: Total 1 entries	Total number of Layer 2 multicast IP forwarding entries in VLAN 2.
(0.0.0.0, 224.1.1.1)	(S, G) entry, where **0.0.0.0** in the S position means all multicast sources.
Host ports (3 in total)	Member ports and total number of member ports.

display l2-multicast mac

Use **display l2-multicast mac** to display information about Layer 2 MAC multicast groups.

Syntax

display l2-multicast mac [*mac-address*] [**vlan** *vlan-id*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

mac-address: Specifies a MAC multicast group by its multicast MAC address. If you do not specify a MAC multicast group, this command displays information about all Layer 2 MAC multicast groups.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays information about Layer 2 MAC multicast groups for all VLANs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about Layer 2 MAC multicast groups for the master device.

Examples

Display information about Layer 2 MAC multicast groups for VLAN 2.

```
<Sysname> display l2-multicast mac vlan 2
Total 1 entries.

VLAN 2: Total 1 entries.
  MAC group address: 0100-5e01-0101
    Attribute: success
    Host ports (1 in total):
      GE1/0/1
```

Table 11 Command output

Field	Description
Total 1 entries	Total number of Layer 2 MAC multicast groups.
VLAN 2: Total 1 entries	Total number of Layer 2 MAC multicast groups in VLAN 2.
MAC group address	Address of the MAC multicast group.
Attribute	Entry attribute: • **success**—Processing has succeeded. • **fail**—Processing has failed.
Host ports (1 in total)	Member ports and total number of member ports.

display l2-multicast mac forwarding

Use **display l2-multicast mac forwarding** to display Layer 2 multicast MAC forwarding entries.

Syntax

display l2-multicast mac forwarding [*mac-address*] [**vlan** *vlan-id*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

mac-address: Specifies a MAC multicast group by its MAC address. If you do not specify a MAC multicast group, this command displays Layer 2 multicast MAC forwarding entries for all MAC multicast groups.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays Layer 2 multicast MAC forwarding entries for all VLANs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays Layer 2 multicast MAC group entries for the master device.

Examples

Display Layer 2 multicast MAC forwarding entries for VLAN 2.

```
<Sysname> display l2-multicast mac forwarding vlan 2
Total 1 entries.

VLAN 2: Total 1 entries.
  MAC group address: 0100-5e01-0101
    Host ports (3 in total):
      GigabitEthernet1/0/1
      GigabitEthernet1/0/2
      GigabitEthernet1/0/3
```

Table 12 Command output

Field	Description
Total 1 entries	Total number of Layer 2 multicast MAC forwarding entries.
VLAN 2: Total 1 entries	Total number of Layer 2 multicast MAC forwarding entries in VLAN 2.
MAC group address	Address of the MAC multicast group.
Host ports (3 in total)	Member ports and total number of member ports.

display mac-address [multicast]

Use **display mac-address** [**multicast**] to display static multicast MAC address entries.

Syntax

display mac-address [*mac-address* [**vlan** *vlan-id*] | [**multicast**] [**vlan** *vlan-id*] [**count**]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

mac-address: Specifies a multicast MAC address. The MAC address can be any legal multicast MAC address except 0100-5Exx-xxxx and 3333-xxxx-xxxx, where "x" represents a hexadecimal number in the range of 0 to F.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays MAC address entries for all VLANs.

multicast: Specifies static multicast MAC address entries.

count: Specifies the number of MAC address entries. If you specify this keyword, the command displays the number of matching MAC address entries. If you do not specify this keyword, the command displays the contents of the matching entries rather than the entry count.

Usage guidelines

If you do not specify any parameters, this command displays all MAC address table entries, including unicast MAC address entries and static multicast MAC address entries.

Examples

Display static multicast MAC address entries for VLAN 2.

```
<Sysname> display mac-address multicast vlan 2
MAC Address      VLAN ID    State            Port/NickName            Aging
0100-0001-0001   2          Multicast        GE1/0/1                  N
```

Display the number of static multicast MAC address entries.

```
<Sysname> display mac-address multicast count
1 mac address(es) found.
```

Table 13 Command output

Field	Description
MAC address	MAC address of a multicast group.
VLAN ID	ID of the VLAN to which the network device identified by the MAC address belongs.
State	Status of the MAC address. If the multicast MAC address entry is static, this field displays **Multicast**.
Port/NickName	Outgoing ports or nickname of the Egress RB in a TRILL network for the packet that is sent to the MAC address in this MAC address entry. TRILL is not supported in the current software version.
Aging	Aging timer state. If this entry never expires, this field displays **N**.
1 mac address(es) found	One static multicast MAC address entry is found.

Related commands

mac-address multicast

dot1p-priority (IGMP-snooping view)

Use **dot1p-priority** to set the 802.1p priority for IGMP messages globally.

Use **undo dot1p-priority** to restore the default.

Syntax

dot1p-priority *priority*

undo dot1p-priority

Default

The global 802.1p priority is 6 for IGMP messages.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

priority: Specifies an 802.1p priority for IGMP messages, in the range of 0 to 7. The greater the value, the higher the priority.

Usage guidelines

You can set the 802.1p priority globally for all VLANs in IGMP-snooping view or for a VLAN in VLAN view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

Examples

Set the 802.1p priority for IGMP messages to 3 globally.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] dot1p-priority 3
```

Related commands

igmp-snooping dot1p-priority

dscp

Use **dscp** to set the DSCP value for outgoing IGMP protocol packets.

Use **undo dscp** to restore the default.

Syntax

dscp *dscp-value*

undo dscp

Default

The DSCP value is 48 for outgoing IGMP protocol packets.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63.

Usage guidelines

The DSCP value is carried in the ToS field of an IP packet to determine the transmission priority of the packet. A greater DSCP value represents a higher priority.

Examples

Set the DSCP value to 63 for outgoing IGMP protocol packets.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] dscp 63
```

enable (IGMP-snooping view)

Use **enable** to enable IGMP snooping for VLANs.

Use **undo enable** to disable IGMP snooping for VLANs.

Syntax

enable vlan *vlan-list*

undo enable vlan *vlan-list*

Default

IGMP snooping status in a VLAN is consistent with the global IGMP snooping status.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094.

Usage guidelines

You must enable the IGMP snooping feature by using the **igmp-snooping** command before you enable IGMP snooping for VLANs.

You can enable IGMP snooping for multiple VLANs by using this command in IGMP-snooping view or for a VLAN by using the **igmp-snooping enable** command in VLAN view. The configuration in IGMP-snooping view has the same priority as the configuration in VLAN view, and the most recent configuration takes effect.

Examples

Enable the IGMP snooping feature, and then enable IGMP snooping for VLAN 2 through VLAN 10.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] enable vlan 2 to 10
```

Related commands

igmp-snooping

igmp-snooping enable

entry-limit (IGMP-snooping view)

Use **entry-limit** to globally set the maximum number of IGMP snooping forwarding entries, including dynamic entries and static entries.

Use **undo entry-limit** to restore the default.

Syntax

entry-limit *limit*

undo entry-limit

Default

The maximum number of IGMP snooping forwarding entries is 4294967295.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

limit: Specifies the maximum number of IGMP snooping forwarding entries, in the range of 0 to 4294967295.

Examples

Set the global maximum number of IGMP snooping forwarding entries to 512.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] entry-limit 512
```

fast-leave (IGMP-snooping view)

Use **fast-leave** to enable fast-leave processing globally.

Use **undo fast-leave** to disable fast-leave processing globally.

Syntax

fast-leave [**vlan** *vlan-list*]

undo fast-leave [**vlan** *vlan-list*]

Default

Fast-leave processing is disabled.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

The fast-leave processing feature enables the device to immediately remove a port from the forwarding entry for a multicast group when the port receives a leave message.

You can enable fast-leave processing globally for all ports in IGMP-snooping view or for a port in interface view. For a port, the port-specific configuration takes priority over the global configuration.

Examples

Globally enable fast-leave processing for VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] fast-leave vlan 2
```

Related commands

igmp-snooping fast-leave

global-enable (IGMP-snooping view)

Use **global-enable** to enable IGMP snooping globally.

Use **undo global-enable** to disable IGMP snooping globally.

Syntax

global-enable

undo global-enable

Default

IGMP snooping is disabled globally.

Views

IGMP-snooping view

Predefined user roles

network-admin

Usage guidelines

To configure other IGMP snooping features for VLANs, you must enable IGMP snooping for the specific VLANs even though IGMP snooping is enabled globally.

Examples

Enable IGMP snooping globally.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] global-enable
```

Related commands

enable (IGMP-snooping view)

igmp-snooping

igmp-snooping disable

igmp-snooping enable

group-policy (IGMP-snooping view)

Use **group-policy** to globally configure a multicast group policy to control the multicast groups that hosts can join.

Use **undo group-policy** to globally delete multicast group policies.

Syntax

group-policy *ipv4-acl-number* [**vlan** *vlan-list*]

undo group-policy [**vlan** *vlan-list*]

Default

No multicast group policies exist. Hosts can join any multicast groups.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

ipv4-acl-number: Specifies an IPv4 basic or advanced ACL by its number in the range of 2000 to 3999. Hosts can join only the multicast groups that the ACL permits. If the ACL does not exist or does not have valid rules, hosts cannot join multicast groups.

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

A multicast group policy filters IGMP reports to control the multicast groups that hosts can join.

This command does not take effect on static member ports, because static member ports do not send IGMP reports.

You can configure a multicast group policy globally for all ports in IGMP-snooping view or for a port in interface view. For a port, the port-specific configuration takes priority over the global configuration.

When you configure a rule in the IPv4 ACL, follow these restrictions and guidelines:

- In a basic ACL, the **source** *source-address source-wildcard* option specifies a multicast group address.
- In an advanced ACL, the **source** *source-address source-wildcard* option specifies a multicast source address. The **destination** *dest-address dest-wildcard* option specifies a multicast group address.

  To match the following IGMP reports, set the **source** *source-address source-wildcard* option to 0.0.0.0:

  - IGMPv1 and IGMPv2 reports.
  - IGMPv3 IS_EX and IGMPv3 TO_EX reports that do not carry multicast source addresses.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

You can configure different ACLs for all ports in different VLANs. If you configure multiple ACLs for all ports in the same VLAN, the most recent configuration takes effect.

Examples

Configure a multicast group policy for VLAN 2 so that hosts in VLAN 2 can join only multicast group 225.1.1.1.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule permit source 225.1.1.1 0
[Sysname-acl-ipv4-basic-2000] quit
[Sysname] igmp-snooping
[Sysname-igmp-snooping] group-policy 2000 vlan 2
```

Related commands

igmp-snooping group-policy

host-aging-time (IGMP-snooping view)

Use **host-aging-time** to set the aging timer for dynamic member ports globally.

Use **undo host-aging-time** to restore the default.

Syntax

host-aging-time *seconds*

undo host-aging-time

Default

The aging timer for dynamic member ports is 260 seconds.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

seconds: Specifies an aging timer for dynamic member ports, in the range of 1 to 8097894 seconds.

Usage guidelines

You can set the timer globally for all VLANs in IGMP-snooping view or for a VLAN in VLAN view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

To avoid mistakenly deleting multicast group members, set the aging timer for dynamic member ports to be greater than the value calculated by using the following formula:

[IGMP general query interval] + [maximum response time for IGMP general queries]

As a best practice, set the aging timer of dynamic member ports to the value calculated by using the following formula:

[IGMP general query interval] × 2 + [maximum response time for IGMP general queries]

Examples

Set the global aging timer for dynamic member ports to 300 seconds.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] host-aging-time 300
```

Related commands

igmp-snooping host-aging-time

host-tracking (IGMP-snooping view)

Use **host-tracking** to enable host tracking globally.

Use **undo host-tracking** to disable host tracking globally.

Syntax

host-tracking

undo host-tracking

Default

Host tracking is disabled.

Views

IGMP-snooping view

Predefined user roles

network-admin

Usage guidelines

You can enable host tracking globally for all VLANs in IGMP-snooping view or for a VLAN in VLAN view. For a VLAN, the global configuration has the same priority as the VLAN-specific configuration.

Examples

Enable host tracking globally.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] host-tracking
```

Related commands

display igmp-snooping host-tracking

igmp-snooping host-tracking

igmp-snooping

Use **igmp-snooping** to enable the IGMP snooping feature and enter IGMP-snooping view.

Use **undo igmp-snooping** to disable the IGMP snooping feature.

Syntax

igmp-snooping

undo igmp-snooping

Default

The IGMP snooping feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

If you disable the IGMP snooping feature, IGMP snooping is disabled in all VLANs.

Examples

Enable the IGMP snooping feature and enter IGMP-snooping view.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping]
```

Related commands

enable (IGMP-snooping view)

igmp-snooping enable

igmp-snooping disable

igmp-snooping access-policy

Use **igmp-snooping access-policy** to configure an IGMP snooping access control policy.

Use **undo igmp-snooping access-policy** to delete an IGMP snooping access control policy.

Syntax

igmp-snooping access-policy *ipv4-acl-number*

undo igmp-snooping access-policy { *ipv4-acl-number* | **all** }

Default

No IGMP snooping access control policies exist. Multicast users can join or leave any multicast groups.

Views

User profile view

Predefined user roles

network-admin

Parameters

ipv4-acl-number: Specifies an IPv4 basic or advanced ACL by its number, in the range of 2000 to 3999. Multicast users can join or leave only the multicast groups that the ACL permits. If the ACL does not exist or does not have valid rules, multicast users cannot join or leave any multicast groups.

all: Specifies all IGMP snooping access control policies.

Usage guidelines

You can repeat this command to configure multiple IGMP snooping access control policies. A multicast user can join or leave a multicast group if its IGMP report or leave message is permitted by one of the IGMP snooping access control policies.

When you configure a rule in the IPv4 ACL, follow these restrictions and guidelines:

- In a basic ACL, the **source** *source-address source-wildcard* option specifies a multicast group address.
- In an advanced ACL, the **source** *source-address source-wildcard* option specifies a multicast source address. The **destination** *dest-address dest-wildcard* option specifies a multicast group address.

  To match the following IGMP messages, set the **source** *source-address source-wildcard* option to 0.0.0.0:

    - IGMPv1 report and leave messages.
    - IGMPv2 report and leave messages.
    - IGMPv3 IS_EX and IGMPv3 TO_EX reports that do not carry multicast source addresses.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

Examples

In user profile **abc**, configure an IGMP snooping access control policy to allow multicast users to join or leave only multicast group 225.1.1.1.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 225.1.1.1 0
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] user-profile abc
[Sysname-user-profile-abc] igmp-snooping access-policy 2001
```

igmp-snooping dot1p-priority

Use **igmp-snooping dot1p-priority** to set the 802.1p priority for IGMP messages in a VLAN.

Use **undo igmp-snooping dot1p-priority** to restore the default.

Syntax

igmp-snooping dot1p-priority *priority*

undo igmp-snooping dot1p-priority

Default

The 802.1p priority is 6 for IGMP messages in a VLAN.

Views

VLAN view

Predefined user roles

network-admin

Parameters

priority: Specifies an 802.1p priority for IGMP messages, in the range of 0 to 7. The greater the value, the higher the priority.

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

You can set the 802.1p priority for a VLAN in VLAN view or globally for all VLANs in IGMP-snooping view. The VLAN-specific configuration takes priority over the global configuration.

Examples

In VLAN 2, enable IGMP snooping, and set the 802.1p priority for IGMP messages to 3.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping dot1p-priority 3
```

Related commands

dot1p-priority (IGMP-snooping view)

enable (IGMP-snooping view)

igmp-snooping enable

igmp-snooping drop-unknown

Use **igmp-snooping drop-unknown** to enable dropping unknown multicast data packets for a VLAN.

Use **undo igmp-snooping drop-unknown** to disable dropping unknown multicast data packets for a VLAN.

Syntax

igmp-snooping drop-unknown

undo igmp-snooping drop-unknown

Default

Dropping unknown multicast data packets is disabled. Unknown multicast data packets are flooded.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

Examples

In VLAN 2, enable IGMP snooping, and enable dropping unknown multicast data packets.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping drop-unknown
```

Related commands

enable (IGMP-snooping view)

igmp-snooping enable

igmp-snooping { disable | enable }

Use **igmp-snooping enable** to enable IGMP snooping for a VLAN.

Use **igmp-snooping disable** to disable IGMP snooping for a VLAN.

Use **undo igmp-snooping** to restore the IGMP snooping status in a VLAN to the global IGMP snooping status.

Syntax

igmp-snooping { **disable** | **enable** }

undo igmp-snooping

Default

The IGMP snooping status in a VLAN is consistent with the global IGMP snooping status.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

You must enable the IGMP snooping feature by using the **igmp-snooping** command before you enable IGMP snooping for a VLAN.

You can enable IGMP snooping for a VLAN by using this command in VLAN view or for multiple VLANs by using the **enable** command in IGMP-snooping view. The configuration in VLAN view has the same priority as the configuration in IGMP-snooping view, and the most recent configuration takes effect.

Examples

Enable the IGMP snooping feature, and then enable IGMP snooping for VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
```

Disable IGMP snooping for VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping disable
```

Related commands

enable (IGMP-snooping view)

igmp-snooping

igmp-snooping fast-leave

Use **igmp-snooping fast-leave** to enable fast-leave processing on a port.

Use **undo igmp-snooping fast-leave** to disable fast-leave processing on a port.

Syntax

igmp-snooping fast-leave [**vlan** *vlan-list*]

undo igmp-snooping fast-leave [**vlan** *vlan-list*]

Default

Fast-leave processing is disabled on a port.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

The fast-leave processing feature enables the device to immediately remove a port from the forwarding entry for a multicast group when the port receives a leave message.

You can enable fast-leave processing for a port in interface view or globally for all ports in IGMP-snooping view. For a port, the port-specific configuration takes priority over the global configuration.

Examples

Enable fast-leave processing for VLAN 2 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping fast-leave vlan 2
```

Related commands

fast-leave (IGMP-snooping view)

igmp-snooping general-query source-ip

Use **igmp-snooping general-query source-ip** to configure the source IP address for IGMP general queries.

Use **undo igmp-snooping general-query source-ip** to restore the default.

Syntax

igmp-snooping general-query source-ip *ip-address*

undo igmp-snooping general-query source-ip

Default

In a VLAN, the source IP address of IGMP general queries is the IP address of the current VLAN interface. If the current VLAN interface does not have an IP address, the source IP address is 0.0.0.0.

Views

VLAN view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the source IP address for IGMP general queries.

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

Examples

In VLAN 2, enable IGMP snooping, and specify 10.1.1.1 as the source IP address of IGMP general queries.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping general-query source-ip 10.1.1.1
```

Related commands

enable (IGMP-snooping view)

igmp-snooping enable

igmp-snooping group-limit

Use **igmp-snooping group-limit** to set the maximum number of multicast groups that a port can join.

Use **undo igmp-snooping group-limit** to remove the limit on the maximum number of multicast groups that a port can join.

Syntax

igmp-snooping group-limit *limit* [**vlan** *vlan-list*]

undo igmp-snooping group-limit [**vlan** *vlan-list*]

Default

No limit is placed on the maximum number of multicast groups that a port can join.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

limit: Specifies the maximum number of multicast groups that a port can join, in the range of 0 to 4294967295.

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

This command takes effect only on the multicast groups that a port joins dynamically.

Examples

On GigabitEthernet 1/0/1, set the maximum number of multicast groups the port can join in VLAN 2 to 10.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping group-limit 10 vlan 2
```

igmp-snooping group-policy

Use **igmp-snooping group-policy** to configure a multicast group policy on a port to control the multicast groups that hosts attached to the port can join.

Use **undo igmp-snooping group-policy** to delete multicast group policies on a port.

Syntax

igmp-snooping group-policy *ipv4-acl-number* [**vlan** *vlan-list*]

undo igmp-snooping group-policy [**vlan** *vlan-list*]

Default

No multicast group polices exist on a port. Hosts attached to the port can join any multicast groups.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

ipv4-acl-number: Specifies an IPv4 basic or advanced ACL by its number in the range of 2000 to 3999. Hosts can join only the multicast groups that the ACL permits. If the ACL does not exist or does not have valid rules, hosts cannot join multicast groups.

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

A multicast group policy filters IGMP reports to control the multicast groups that hosts can join.

This command does not take effect on static member ports, because static member ports do not send IGMP reports.

You can configure a multicast group policy for a port in interface view or globally for all ports in IGMP-snooping view. For a port, the port-specific configuration takes priority over the global configuration.

When you configure a rule in the IPv4 ACL, follow these restrictions and guidelines:

- In a basic ACL, the **source** *source-address source-wildcard* option specifies a multicast group address.
- In an advanced ACL, the **source** *source-address source-wildcard* option specifies a multicast source address. The **destination** *dest-address dest-wildcard* option specifies a multicast group address.

  To match the following IGMP reports, set the **source** *source-address source-wildcard* option to 0.0.0.0:

  - IGMPv1 and IGMPv2 reports.
  - IGMPv3 IS_EX and IGMPv3 TO_EX reports that do not carry multicast source addresses.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

You can configure different ACLs on a port for different VLANs. If you configure multiple ACLs on a port for the same VLAN, the most recent configuration takes effect.

Examples

On GigabitEthernet 1/0/1, configure a multicast group policy for VLAN 2 so that hosts in VLAN 2 can join only multicast group 225.1.1.1.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule permit source 225.1.1.1 0
[Sysname-acl-ipv4-basic-2000] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping group-policy 2000 vlan 2
```

Related commands

group-policy (IGMP-snooping view)

igmp-snooping host-aging-time

Use **igmp-snooping host-aging-time** to set the aging timer for dynamic member ports in a VLAN.

Use **undo igmp-snooping host-aging-time** to restore the default.

Syntax

igmp-snooping host-aging-time *seconds*

undo igmp-snooping host-aging-time

Default

The aging timer for dynamic member ports is 260 seconds.

Views

VLAN view

Predefined user roles

network-admin

Parameters

seconds: Specifies an aging timer for dynamic member ports, in the range of 1 to 8097894 seconds.

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

You can set the timer for a VLAN in VLAN view or globally for all VLANs in IGMP-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

To avoid mistakenly deleting multicast group members, set the aging timer for dynamic member ports to be greater than the value calculated by using the following formula:

[IGMP general query interval] + [maximum response time for IGMP general queries]

As a best practice, set the aging timer of dynamic member ports to the value calculated by using the following formula:

[IGMP general query interval] × 2 + [maximum response time for IGMP general queries]

Examples

In VLAN 2, enable IGMP snooping, and set the aging timer for dynamic member ports to 300 seconds.

```
<Sysname> system-view
```

```
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping host-aging-time 300
```

Related commands

enable (IGMP-snooping view)

host-aging-time (IGMP-snooping view)

igmp-snooping enable

igmp-snooping host-join

Use **igmp-snooping host-join** to configure a port as a simulated member host for a multicast group.

Use **undo igmp-snooping host-join** to remove the configuration of a simulated member host for a multicast group.

Syntax

igmp-snooping host-join *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*

undo igmp-snooping host-join { *group-address* [**source-ip** *source-address*] **vlan** *vlan-id* | **all** }

Default

A port is not configured as a simulated member host for multicast groups.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

group-address: Specifies a multicast group in the range of 224.0.1.0 to 239.255.255.255.

source-ip *source-address*: Specifies a multicast source by its IP address. If you specify a multicast source, this command configures the port as a simulated member host for a multicast source and group. If you do not specify a multicast source, this command configures the port as a simulated member host for a multicast group. This option takes effect on IGMPv3 snooping devices.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

all: Specifies all multicast groups.

Usage guidelines

The version of IGMP running on a simulated member host is the same as the version of IGMP snooping running on the port. The port ages out in the same way as a dynamic member port.

Examples

Configure GigabitEthernet 1/0/1 as a simulated member host of the multicast source and group (1.1.1.1, 232.1.1.1) in VLAN 2.

```
<Sysname> system-view
```

```
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping version 3
[Sysname-vlan2] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping host-join 232.1.1.1 source-ip 1.1.1.1 vlan
2
```

igmp-snooping host-tracking

Use **igmp-snooping host-tracking** to enable host tracking for a VLAN.

Use **undo igmp-snooping host-tracking** to disable host tracking for a VLAN.

Syntax

igmp-snooping host-tracking

undo igmp-snooping host-tracking

Default

Host tracking is disabled.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command for the VLAN.

You can enable host tracking for a VLAN in VLAN view or globally for all VLANs in IGMP-snooping view. For a VLAN, the VLAN-specific configuration has the same priority as the global configuration.

Examples

In VLAN 2, enable IGMP snooping, and then enable host tracking.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping host-tracking
```

Related commands

display igmp-snooping host-tracking

host-tracking (IGMP-snooping view)

igmp-snooping enable

igmp-snooping last-member-query-interval

Use **igmp-snooping last-member-query-interval** to set the IGMP last member query interval for a VLAN.

Use **undo igmp-snooping last-member-query-interval** to restore the default.

Syntax

igmp-snooping last-member-query-interval *interval*

undo igmp-snooping last-member-query-interval

Default

The IGMP last member query interval is 1 second.

Views

VLAN view

Predefined user roles

network-admin

Parameters

interval: Specifies an IGMP last member query interval in the range of 1 to 25 seconds.

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

You can set the interval for a VLAN in VLAN view or globally for all VLANs in IGMP-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

Examples

In VLAN 2, enable IGMP snooping, and set the IGMP last member query interval to 3 seconds.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping last-member-query-interval 3
```

Related commands

enable (IGMP-snooping view)

igmp-snooping enable

last-member-query-interval (IGMP-snooping view)

igmp-snooping leave source-ip

Use **igmp-snooping leave source-ip** to configure the source IP address for IGMP leave messages.

Use **undo igmp-snooping leave source-ip** to restore the default.

Syntax

igmp-snooping leave source-ip *ip-address*

undo igmp-snooping leave source-ip

Default

In a VLAN, the source IP address of IGMP leave messages is the IP address of the current VLAN interface. If the current VLAN interface does not have an IP address, the source IP address is 0.0.0.0.

Views

VLAN view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the source IP address for IGMP leave messages.

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

Examples

In VLAN 2, enable IGMP snooping, and specify 10.1.1.1 as the source IP address of IGMP leave messages.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping leave source-ip 10.1.1.1
```

Related commands

enable (IGMP-snooping view)

igmp-snooping enable

igmp-snooping max-response-time

Use **igmp-snooping max-response-time** to set the maximum response time for IGMP general queries in a VLAN.

Use **undo igmp-snooping max-response-time** to restore the default.

Syntax

igmp-snooping max-response-time *seconds*

undo igmp-snooping max-response-time

Default

The maximum response time for IGMP general queries is 10 seconds.

Views

VLAN view

Predefined user roles

network-admin

Parameters

seconds: Specifies the maximum response time for IGMP general queries, in the range of 1 to 3174 seconds.

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

You can set the time for a VLAN in VLAN view or globally for all VLANs in IGMP-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

To avoid mistakenly deleting multicast group members, set the maximum response time for IGMP general queries to be less than the IGMP general query interval.

Examples

In VLAN 2, enable IGMP snooping, and set the maximum response time for IGMP general queries to 5 seconds.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping max-response-time 5
```

Related commands

enable (IGMP-snooping view)

igmp-snooping enable

igmp-snooping query-interval

max-response-time (IGMP-snooping view)

igmp-snooping overflow-replace

Use **igmp-snooping overflow-replace** to enable multicast group replacement on a port.

Use **undo igmp-snooping overflow-replace** to disable multicast group replacement on a port.

Syntax

igmp-snooping overflow-replace [**vlan** *vlan-list*]

undo igmp-snooping overflow-replace [**vlan** *vlan-list*]

Default

Multicast group replacement is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

This command takes effect only on the multicast groups that a port joins dynamically.

You can enable multicast group replacement for a port in interface view or globally for all ports in IGMP-snooping view. For a port, the port-specific configuration takes priority over the global configuration.

Examples

On GigabitEthernet 1/0/1, enable multicast group replacement for VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping overflow-replace vlan 2
```

Related commands

overflow-replace (IGMP-snooping view)

igmp-snooping proxy enable

Use **igmp-snooping proxy enable** to enable IGMP snooping proxying for a VLAN.

Use **undo igmp-snooping proxy enable** to disable IGMP snooping proxying for a VLAN.

Syntax

igmp-snooping proxy enable

undo igmp-snooping proxy enable

Default

IGMP snooping proxying is disabled.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

This command does not take effect on a VLAN that is a sub-VLAN of a multicast VLAN.

Examples

In VLAN 2, enable IGMP snooping, and enable IGMP snooping proxying.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping proxy enable
```

Related commands

enable (IGMP-snooping view)

igmp-snooping enable

subvlan (multicast-VLAN view)

igmp-snooping querier

Use **igmp-snooping querier** to enable the IGMP snooping querier.

Use **undo igmp-snooping querier** to disable the IGMP snooping querier.

Syntax

igmp-snooping querier

undo igmp-snooping querier

Default

The IGMP snooping querier is disabled.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

For a sub-VLAN of a multicast VLAN, this command takes effect only after you remove the sub-VLAN from the multicast VLAN.

Examples

In VLAN 2, enable IGMP snooping, and enable the IGMP snooping querier.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping querier
```

Related commands

enable (IGMP-snooping view)

igmp-snooping enable

subvlan (multicast VLAN view)

igmp-snooping querier-election

Use **igmp-snooping querier-election** to enable IGMP snooping querier election for a VLAN.

Use **undo igmp-snooping querier-election** to disable IGMP snooping querier election for a VLAN.

Syntax

igmp-snooping querier-election

undo igmp-snooping querier-election

Default

IGMP snooping querier election is disabled for a VLAN.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

For IGMP snooping querier election to take effect, you must enable the IGMP snooping querier.

Examples

In VLAN 2, enable IGMP snooping, and enable IGMP snooping querier election.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping querier
[Sysname-vlan2] igmp-snooping querier-election
```

Related commands

igmp-snooping querier

igmp-snooping query-interval

Use **igmp-snooping query-interval** to set the IGMP general query interval for a VLAN.

Use **undo igmp-snooping query-interval** to restore the default.

Syntax

igmp-snooping query-interval *interval*

undo igmp-snooping query-interval

Default

The IGMP general query interval is 125 seconds.

Views

VLAN view

Predefined user roles

network-admin

Parameters

interval: Specifies an IGMP general query interval in the range of 2 to 31744 seconds.

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

To avoid mistakenly deleting multicast group members, set the IGMP general query interval to be greater than the maximum response time for IGMP general queries.

Examples

In VLAN 2, enable IGMP snooping, and set the IGMP general query interval to 20 seconds.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping query-interval 20
```

Related commands

enable (IGMP-snooping view)

igmp-snooping enable

igmp-snooping max-response-time

igmp-snooping querier

max-response-time

igmp-snooping report source-ip

Use **igmp-snooping report source-ip** to configure the source IP address for IGMP reports.

Use **undo igmp-snooping report source-ip** to restore the default.

Syntax

igmp-snooping report source-ip *ip-address*

undo igmp-snooping report source-ip

Default

In a VLAN, the source IP address of IGMP reports is the IP address of the current VLAN interface. If the current VLAN interface does not have an IP address, the source IP address is 0.0.0.0.

Views

VLAN view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the source IP address for IGMP reports.

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

Examples

In VLAN 2, enable IGMP snooping, and specify 10.1.1.1 as the source IP address of IGMP reports.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping report source-ip 10.1.1.1
```

Related commands

enable (IGMP-snooping view)

igmp-snooping enable

igmp-snooping router-aging-time

Use **igmp-snooping router-aging-time** to set the aging timer for dynamic router ports in a VLAN.

Use **undo igmp-snooping router-aging-time** to restore the default.

Syntax

igmp-snooping router-aging-time *seconds*

undo igmp-snooping router-aging-time

Default

The aging timer for dynamic router ports is 260 seconds.

Views

VLAN view

Predefined user roles

network-admin

Parameters

seconds: Specifies an aging timer for dynamic router ports, in the range of 1 to 8097894 seconds.

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

You can set the timer for a VLAN in VLAN view or globally for all VLANs in IGMP-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

Examples

In VLAN 2, enable IGMP snooping, and set the aging timer for dynamic router ports to 100 seconds.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping router-aging-time 100
```

Related commands

enable (IGMP-snooping view)

igmp-snooping enable

router-aging-time (IGMP-snooping view)

igmp-snooping router-port-deny

Use **igmp-snooping router-port-deny** to disable a port from becoming a dynamic router port.

Use **undo igmp-snooping router-port-deny** to allow a port to become a dynamic router port.

Syntax

igmp-snooping router-port-deny [**vlan** *vlan-list*]

undo igmp-snooping router-port-deny [**vlan** *vlan-list*]

Default

A port is allowed to become a dynamic router port.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you specify VLANs, this command takes effect only when the port belongs to the specified VLANs. If you do not specify a VLAN, this command takes effect on all VLANs to which the port belongs.

Examples

Disable GigabitEthernet 1/0/1 from becoming a dynamic router port in VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping router-port-deny vlan 2
```

igmp-snooping source-deny

Use **igmp-snooping source-deny** to enable multicast source port filtering on a port to discard all multicast data packets.

Use **undo igmp-snooping source-deny** to disable multicast source port filtering on a port.

Syntax

igmp-snooping source-deny

undo igmp-snooping source-deny

Default

Multicast source port filtering is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

You can enable this feature for a port in interface view or for the specified ports in IGMP-snooping view. For a port, the configuration in interface view has the same priority as the configuration in IGMP-snooping view, and the most recent configuration takes effect.

Examples

Enable source port filtering for multicast data on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping source-deny
```

Related commands

source-deny (IGMP-snooping view)

igmp-snooping special-query source-ip

Use **igmp-snooping special-query source-ip** to configure the source IP address for IGMP group-specific queries.

Use **undo igmp-snooping special-query source-ip** to restore the default.

Syntax

igmp-snooping special-query source-ip *ip-address*

undo igmp-snooping special-query source-ip

Default

In a VLAN, the source IP address of IGMP group-specific queries is one of the following:

- The source address of IGMP group-specific queries if the IGMP snooping querier of the VLAN has received IGMP general queries.
- The IP address of the current VLAN interface if the IGMP snooping querier does not receive an IGMP general query.
- 0.0.0.0 if the IGMP snooping querier does not receive an IGMP general query and the current VLAN interface does not have an IP address.

Views

VLAN view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the source IP address for IGMP group-specific queries.

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

Examples

In VLAN 2, enable IGMP snooping, and specify 10.1.1.1 as the source IP address of IGMP group-specific queries.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping special-query source-ip 10.1.1.1
```

Related commands

enable (IGMP-snooping view)

igmp-snooping enable

igmp-snooping static-group

Use **igmp-snooping static-group** to configure a port as a static member port of a multicast group.

Use **undo igmp-snooping static-group** to remove the configuration of static member ports.

Syntax

igmp-snooping static-group *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*

undo igmp-snooping static-group { *group-address* [**source-ip** *source-address*] **vlan** *vlan-id* | **all** }

Default

A port is not a static member port of a multicast group.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

group-address: Specifies a multicast group address in the range of 224.0.1.0 to 239.255.255.255.

source-ip *source-address*: Specifies a multicast source by its IP address. If you specify a multicast source, this command configures the port as a static member port for a multicast source and group. If you do not specify a multicast source, this command configures the port as a static member port for a multicast group. This option takes effect on IGMPv3 snooping devices.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

all: Specifies all multicast groups.

Examples

Configure GigabitEthernet 1/0/1 as a static member port of the multicast source and group (1.1.1.1, 225.0.0.1) in VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping version 3
[Sysname-vlan2] quit
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping static-group 225.0.0.1 source-ip 1.1.1.1
vlan 2
```

igmp-snooping static-router-port

Use **igmp-snooping static-router-port** to configure a port as a static router port.

Use **undo igmp-snooping static-router-port** to remove the configuration of static router ports.

Syntax

igmp-snooping static-router-port vlan *vlan-id*

undo igmp-snooping static-router-port { **all** | **vlan** *vlan-id* }

Default

A port is not a static router port.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

all: Specifies all VLANs.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

Examples

Configure GigabitEthernet 1/0/1 as a static router port in VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping static-router-port vlan 2
```

igmp-snooping version

Use **igmp-snooping version** to specify an IGMP snooping version for a VLAN.

Use **undo igmp-snooping version** to restore the default.

Syntax

igmp-snooping version *version-number*

undo igmp-snooping version

Default

The IGMP snooping version in a VLAN is 2.

Views

VLAN view

Predefined user roles

network-admin

Parameters

version-number: Specifies an IGMP snooping version, 2 or 3.

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

You can specify the version for a VLAN in VLAN view or for the specified VLANs in IGMP-snooping view. The VLAN-specific configuration has the same priority as the configuration in IGMP-snooping view, and the most recent configuration takes effect.

Examples

In VLAN 2, enable IGMP snooping, and specify IGMP snooping version 3.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping version 3
```

Related commands

enable (IGMP-snooping view)

igmp-snooping enable

version (IGMP-snooping view)

last-member-query-interval (IGMP-snooping view)

Use **last-member-query-interval** to set the IGMP last member query interval globally.

Use **undo last-member-query-interval** to restore the default.

Syntax

last-member-query-interval *interval*

undo last-member-query-interval

Default

The IGMP last member query interval is 1 second.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

interval: Specifies an IGMP last member query interval in the range of 1 to 25 seconds.

Usage guidelines

You can set the interval for a VLAN in VLAN view or globally for all VLANs in IGMP-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

Examples

Set the global IGMP last member query interval to 3 seconds.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] last-member-query-interval 3
```

Related commands

igmp-snooping last-member-query-interval

mac-address multicast

Use **mac-address multicast** to configure a static multicast MAC address entry.

Use **undo mac-address multicast** to delete a static multicast MAC address entry.

Syntax

In system view:

mac-address multicast *mac-address* **interface** *interface-list* **vlan** *vlan-id*

undo mac-address [**multicast**] [[*mac-address* [**interface** *interface-list*]] **vlan** *vlan-id*]

In Layer 2 aggregate interface view or Layer 2 Ethernet interface view:

mac-address multicast *mac-address* **vlan** *vlan-id*

undo mac-address [**multicast**] *mac-address* **vlan** *vlan-id*

Default

No static multicast MAC address entries exist.

Views

System view

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

mac-address: Specifies a static multicast MAC address, in the format of H-H-H. You must specify an unused multicast MAC address. A multicast MAC address is a MAC address in which the least significant bit of the most significant octet is 1.

interface *interface-list*: Specifies a space-separated list of up to four interface items. Each item specifies an interface or an interface list in the format of *start-interface-type interface-number* **to** *end-interface-type interface-number*. The *interface-type interface-number* argument specifies an interface by its type and number. The available interface types include Layer 2 Ethernet interfaces and Layer 2 aggregate interfaces.

vlan *vlan-id*: Specifies an existing VLAN by its VLAN ID in the range of 1 to 4094. The system gives a prompt if the specified interface does not belong to the VLAN.

Usage guidelines

You do not need to enable IP multicast routing before you execute this command.

You can configure static multicast MAC address entries for the specified interfaces in system view or for the current interface in interface view.

If you do not specify the **multicast** keyword in the **undo mac-address** command, all static unicast MAC address entries and static multicast MAC entries are deleted.

Examples

Configure a static multicast MAC address entry. In the entry, the multicast MAC address is 0100-5E00-0003 and the outgoing ports are GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5 in VLAN 2.

```
<Sysname> system-view
[Sysname] mac-address multicast 0100-5e00-0003 interface gigabitethernet 1/0/1 to
gigabitethernet 1/0/5 vlan 2
```

Configure a static multicast MAC address entry on GigabitEthernet 1/0/1. In the entry, the multicast MAC address is 0100-5E00-0003 and the outgoing port is GigabitEthernet 1/0/1, which belongs to VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-address multicast 0100-5e00-0003 vlan 2
```

Related commands

display mac-address multicast

max-response-time (IGMP-snooping view)

Use **max-response-time** to set the maximum response time for IGMP general queries globally.

Use **undo max-response-time** to restore the default.

Syntax

max-response-time *seconds*

undo max-response-time

Default

The maximum response time for IGMP general queries is 10 seconds.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

seconds: Specifies the maximum response time for IGMP general queries, in the range of 1 to 3174 seconds.

Usage guidelines

You can set the time for a VLAN in VLAN view or globally for all VLANs in IGMP-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

To avoid mistakenly deleting multicast group members, set the maximum response time for IGMP general queries to be less than the IGMP general query interval.

Examples

Set the global maximum response time for IGMP general queries to 5 seconds.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] max-response-time 5
```

Related commands

igmp-snooping max-response-time

igmp-snooping query-interval

overflow-replace (IGMP-snooping view)

Use **overflow-replace** to enable the multicast group replacement feature globally.

Use **undo overflow-replace** to disable the multicast group replacement feature globally.

Syntax

overflow-replace [**vlan** *vlan-list*]

undo overflow-replace [**vlan** *vlan-list*]

Default

The multicast group replacement feature is disabled.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

This command takes effect only on the multicast groups that a port joins dynamically.

You can enable the multicast group replacement feature globally for all ports in IGMP-snooping view or for a port in interface view. For a port, the port-specific configuration takes priority over the global configuration.

Examples

Globally enable the multicast group replacement feature for VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] overflow-replace vlan 2
```

Related commands

igmp-snooping overflow-replace

report-aggregation (IGMP-snooping view)

Use **report-aggregation** to enable IGMP report suppression.

Use **undo report-aggregation** to disable IGMP report suppression.

Syntax

report-aggregation

undo report-aggregation

Default

IGMP report suppression is enabled.

Views

IGMP-snooping view

Predefined user roles

network-admin

Examples

Disable IGMP report suppression.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] undo report-aggregation
```

reset igmp-snooping group

Use **reset igmp-snooping group** to clear information about dynamic IGMP snooping group entries.

Syntax

reset igmp-snooping group { *group-address* [*source-address*] | **all** } [**vlan** *vlan-id*]

Views

User view

Predefined user roles

network-admin

Parameters

group-address: Specifies a multicast group address in the range of 224.0.1.0 to 239.255.255.255.

source-address: Specifies a multicast source address. If you do not specify a multicast source, this command clears information about dynamic IGMP snooping group entries for all multicast sources.

all: Specifies all multicast groups.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command clears information about dynamic IGMP snooping group entries for all VLANs.

Examples

Clear information about all dynamic IGMP snooping group entries.

```
<Sysname> reset igmp-snooping group all
```

Related commands

display igmp-snooping group

reset igmp-snooping router-port

Use **reset igmp-snooping router-port** to clear dynamic router port information.

Syntax

reset igmp-snooping router-port { **all** | **vlan** *vlan-id* }

Views

User view

Predefined user roles

network-admin

Parameters

all: Specifies all dynamic router ports.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command clears dynamic router port information for all VLANs.

Examples

Clear dynamic router port information.

```
<Sysname> reset igmp-snooping router-port all
```

Related commands

display igmp-snooping router-port

reset igmp-snooping statistics

Use **reset igmp-snooping statistics** to clear statistics for IGMP messages and PIMv2 hello messages learned through IGMP snooping.

Syntax

reset igmp-snooping statistics

Views

User view

Predefined user roles

network-admin

Examples

Clear the statistics for all IGMP messages and PIMv2 hello messages learned through IGMP snooping.

```
<Sysname> reset igmp-snooping statistics
```

Related commands

display igmp-snooping statistics

reset l2-multicast fast-forwarding cache

Use **reset l2-multicast fast-forwarding cache** to clear Layer 2 multicast fast forwarding entries.

Syntax

reset l2-multicast fast-forwarding cache [**vlan** *vlan-id*] { { *source-address* | *group-address* } * | **all** } [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

Parameters

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

source-address: Specifies a multicast source address.

group-address: Specifies a multicast group address in the range of 224.0.1.0 to 239.255.255.255.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears Layer 2 multicast fast forwarding entries for the master device.

all: Specifies all Layer 2 multicast fast forwarding entries.

Examples

Clear all Layer 2 multicast fast forwarding entries.

```
<Sysname> reset l2-multicast fast-forwarding cache all
```

Clear the Layer 2 multicast fast forwarding entry for the multicast source and group (20.0.0.2, 225.0.0.2).

```
<Sysname> reset l2-multicast fast-forwarding cache 20.0.0.2 225.0.0.2
```

Related commands

display l2-multicast fast-forwarding cache

router-aging-time (IGMP-snooping view)

Use **router-aging-time** to set the aging timer for dynamic router ports globally.

Use **undo router-aging-time** to restore the default.

Syntax

router-aging-time *seconds*

undo router-aging-time

Default

The aging timer for dynamic router ports is 260 seconds.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

seconds: Specifies an aging timer for dynamic router ports, in the range of 1 to 8097894 seconds.

Usage guidelines

You can set the timer globally for all VLANs in IGMP-snooping view or for a VLAN in VLAN view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

Examples

Set the global aging timer for dynamic router ports to 100 seconds.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] router-aging-time 100
```

Related commands

igmp-snooping router-aging-time

source-deny (IGMP-snooping view)

Use **source-deny** to enable multicast source port filtering on ports to discard all multicast data packets.

Use **undo source-deny** to disable multicast source port filtering on ports.

Syntax

source-deny port *interface-list*

undo source-deny port *interface-list*

Default

Multicast source port filtering is disabled.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

port *interface-list*: Specifies a space-separated list of port items. Each item specifies a port by its port type and number or a range of ports in the form of *start-interface-type interface-number* **to** *end-interface-type interface-number*.

Usage guidelines

You can enable this feature for the specified ports in IGMP-snooping view or for a port in interface view. For a port, the configuration in IGMP-snooping view has the same priority as the configuration in interface view, and the most recent configuration takes effect.

Examples

Enable multicast source port filtering on ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] source-deny port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

Related commands

igmp-snooping source-deny

version (IGMP-snooping view)

Use **version** to specify an IGMP snooping version for VLANs.

Use **undo version** to restore the default.

Syntax

version *version-number* **vlan** *vlan-list*

undo version vlan *vlan-list*

Default

The IGMP snooping version in a VLAN is 2.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

version-number: Specifies an IGMP snooping version, 2 or 3.

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094.

Usage guidelines

You must enable IGMP snooping for the specified VLANs before you execute this command.

You can specify the version for the specified VLANs in IGMP-snooping view or for a VLAN in VLAN view. The configuration in IGMP-snooping view has the same priority as the VLAN-specific configuration, and the most recent configuration takes effect.

Examples

Enable IGMP snooping for VLAN 2 through VLAN 10, and specify IGMP snooping version 3 for these VLANs.

```
<Sysname> system-view
```

```
[Sysname] igmp-snooping
[Sysname-igmp-snooping] enable vlan 2 to 10
[Sysname-igmp-snooping] version 3 vlan 2 to 10
```

Related commands

enable (IGMP-snooping view)

igmp-snooping enable

igmp-snooping version

Contents

PIM snooping commands

display pim-snooping neighbor

Use **display pim-snooping neighbor** to display PIM snooping neighbor information.

Syntax

display pim-snooping neighbor [**vlan** *vlan-id*] [**slot** *slot-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays PIM snooping neighbor information for all VLANs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays PIM snooping neighbor information for the master device.

verbose: Displays detailed information about PIM snooping neighbors. If you do not specify this keyword, the command displays brief information about PIM snooping neighbors.

Examples

Display detailed information about PIM snooping neighbors for VLAN 2.

```
<Sysname> display pim-snooping neighbor vlan 2 verbose
Total 2 neighbors.

VLAN 2: Total 2 neighbors.
  10.1.1.2
    Slots (0 in total):
    Ports (1 in total):
      GE1/0/1                          (02:02:23)    LAN Prune Delay(T)
  10.1.1.3
    Slots (0 in total):
    Ports (1 in total):
      GE1/0/2                          (02:02:25)
```

Table 1 Command output

Field	Description
Total 2 neighbors	Total number of PIM snooping neighbors.
VLAN 2: Total 2 neighbors	Total number of PIM snooping neighbors in VLAN 2.
10.1.1.2	IP address of the PIM snooping neighbor.
Slots (0 in total)	Member IDs and total number of the member devices that have the neighbor, except for the specified member device or the master device

Field	Description
	when no member device is specified.
Ports (1 in total)	Ports where the PIM snooping neighbors reside, and the total number of the ports.
(02:02:23)	Remaining aging timer for a PIM snooping neighbor on the port. This field is always displayed for global ports (such as Layer 2 aggregate interfaces). For a non-global port, this field is displayed when one of the following conditions exists: • The port is on the specified member device. • The port is on the master device and no member device is specified.
LAN Prune Delay	The PIM hello message sent by the PIM snooping neighbor has the LAN_Prune_Delay option.
(T)	The join message suppression feature has been disabled for the PIM snooping neighbor.

display pim-snooping router-port

Use **display pim-snooping router-port** to display PIM snooping router port information.

Syntax

display pim-snooping router-port [**vlan** *vlan-id*] [**slot** *slot-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays PIM snooping router port information for all VLANs.

verbose: Displays detailed information about PIM snooping router ports. If you do not specify this keyword, the command displays brief information about PIM snooping router ports.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays PIM snooping router port information for the master device.

Examples

Display brief information about PIM snooping router ports for VLAN 2.

```
<Sysname> display pim-snooping router-port vlan 2
VLAN 2:
  Router ports (2 in total):
    GE1/0/1                                 (00:01:30)
    GE1/0/2                                 (00:01:32)
```

Display detailed information about PIM snooping router ports for VLAN 2.

```
<Sysname> display pim-snooping router-port vlan 2 verbose
VLAN 2:
```

```
  Router slots (0 in total):
  Router ports (2 in total):
    GE1/0/1                           (00:01:30)
    GE1/0/2                           (00:01:32)
```

Table 2 Command output

Field	Description
VLAN 2	VLAN ID.
Router slots (0 in total)	Member IDs and total number of the member devices that have router ports, except for the specified member device or the master device when no member device is specified.
Router ports (2 in total)	Router ports and total number of router ports.
(00:01:30)	Remaining aging time for the router port. For a global port, this field is always displayed. For a non-global port, this field is displayed when one of the following conditions exists: • The port is on the specified member device. • The port is on the master device and no member device is specified.

display pim-snooping routing-table

Use **display pim-snooping routing-table** to display PIM snooping routing entries.

Syntax

display pim-snooping routing-table [**vlan** *vlan-id*] [**slot** *slot-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays PIM snooping routing entries for all VLANs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays PIM snooping routing entries for the master device.

verbose: Displays detailed information about PIM snooping routing entries. If you do not specify the keyword, this command displays brief information about PIM snooping routing entries.

Examples

Display detailed information about PIM snooping routing entries for VLAN 2.

```
<Sysname> display pim-snooping routing-table vlan 2 verbose
Total 1 entries.
FSM Flag: NI-no info, J-join, PP-prune pending

VLAN 2: Total 1 entries.
```

```
(172.10.10.1, 225.1.1.1)
  FSM information: dummy
  Upstream neighbor: 20.1.1.1
    Upstream Slots (0 in total):
    Upstream Ports (1 in total):
      GE1/0/1
    Downstream Slots (0 in total):
    Downstream Ports (2 in total):
      GE1/0/2
        Expires: 00:03:01, FSM: J
        Downstream Neighbors (2 in total):
          7.1.1.1
            Expires: 00:59:19, FSM: J
          7.1.1.11
            Expires: 00:59:20, FSM: J
      GE1/0/3
        Expires: 00:02:21, FSM: PP
```

Table 3 Command output

Field	Description
Total 1 entries	Total number of (S, G) entries and (*, G) entries.
FSM Flag: NI-no info, J-join, PP-prune pending	State machine flag of the downstream port: • **NI**—Initial state. • **J**—Join. • **PP**—Prune pending.
VLAN 2: Total 1 entries	Total number of (S, G) entries and (*, G) entries in VLAN 2.
(172.10.10.1, 225.1.1.1)	(S, G) entry.
FSM information	Finite state machine information of the entry: • **delete**—The entry attributes have been deleted. • **dummy**—The entry is a new temporary entry. • **no info**—The entry does not exist. • **normal**—The entry is a correct entry.
Upstream neighbor	Upstream neighbor of the (S, G) or (*, G) entry.
Upstream Slots (0 in total)	Member IDs and total number of the member devices that have the upstream neighbor, except for the specified member device or the master device when no member device is specified.
Upstream Ports (1 in total)	Upstream ports, and the total number of upstream ports. This field is displayed when one of the following conditions exists: • The port is on the specified member device. • The port is on the master device and no member device is specified.
Downstream Slots (0 in total)	Member IDs and total number of the member devices that have downstream ports, except for the specified member device or the master device when no member device is specified.
Downstream Ports (2 in total)	Downstream ports of the upstream neighbor, and the total number of the downstream ports.
Downstream Neighbors (2 in total)	Downstream neighbors of the downstream port, and the total number of the downstream neighbors.

Field	Description
Expires: 00:03:01, FSM: J	Remaining aging time for the downstream port or downstream neighbor, and the finite state machine information. For a global port, this field is always displayed. For a non-global port, this field is displayed when one of the following conditions exists: • The port is on the specified member device. • The port is on the master device and no member device is specified.

display pim-snooping statistics

Use **display pim-snooping statistics** to display statistics for the PIM messages learned through PIM snooping.

Syntax

display pim-snooping statistics

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display statistics for the PIM messages learned through PIM snooping.

```
<Sysname> display pim-snooping statistics
Received PIMv2 hello:  100
Received PIMv2 join/prune:  100
Received PIMv2 error:  0
Received PIMv2 messages in total:  200
Received PIMv1 messages in total:  0
```

Table 4 Command output

Field	Description
Received PIMv2 hello	Number of received PIMv2 hello messages.
Received PIMv2 join/prune	Number of received PIMv2 join/prune messages.
Received PIMv2 error	Number of received PIMv2 messages with errors.
Received PIMv2 messages in total	Total number of received PIMv2 messages.
Received PIMv1 messages in total	Total number of received PIMv1 messages.

Related commands

reset pim-snooping statistics

pim-snooping enable

Use **pim-snooping enable** to enable PIM snooping for a VLAN.

Use **undo pim-snooping enable** to disable PIM snooping for a VLAN.

Syntax

pim-snooping enable

undo pim-snooping enable

Default

PIM snooping is disabled for a VLAN.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

You must enable the IGMP snooping feature and enable IGMP snooping for a VLAN before you enable PIM snooping for the VLAN.

PIM snooping does not take effect on sub-VLANs of a multicast VLAN.

Examples

Enable the IGMP snooping feature, and then enable IGMP snooping and PIM snooping for VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] pim-snooping enable
```

Related commands

igmp-snooping

igmp-snooping enable

pim-snooping graceful-restart join-aging-time

Use **pim-snooping graceful-restart join-aging-time** to set the aging time for global downstream ports and global router ports on the new master device after a master/subordinate switchover.

Use **undo pim-snooping graceful-restart join-aging-time** to restore the default.

Syntax

pim-snooping graceful-restart join-aging-time *seconds*

undo pim-snooping graceful-restart join-aging-time

Default

The aging time is 210 seconds for global downstream ports and global router ports on the new master device after a master/subordinate switchover.

Views

VLAN view

Predefined user roles

network-admin

Parameters

seconds: Specifies an aging time in the range of 210 to 18000 seconds.

Usage guidelines

You must enable PIM snooping for a VLAN before you execute this command.

Global ports include Layer 2 aggregate interfaces. A global downstream port or a global router port is a global port that acts as a downstream port or router port, respectively.

Examples

In VLAN 2, set the aging time to 600 seconds for global downstream ports and global router ports on the new master device after a master/subordinate switchover.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] pim-snooping enable
[Sysname-vlan2] pim-snooping graceful-restart join-aging-time 600
```

Related commands

pim-snooping enable

pim-snooping graceful-restart neighbor-aging-time

Use **pim-snooping graceful-restart neighbor-aging-time** to set the aging time for global neighbor ports on the new master device after a master/subordinate switchover.

Use **undo pim-snooping graceful-restart neighbor-aging-time** to restore the default.

Syntax

pim-snooping graceful-restart neighbor-aging-time *seconds*

undo pim-snooping graceful-restart neighbor-aging-time

Default

The aging time is 105 seconds for global neighbor ports on the new master device after a master/subordinate switchover.

Views

VLAN view

Predefined user roles

network-admin

Parameters

seconds: Specifies an aging time in the range of 105 to 18000 seconds.

Usage guidelines

You must enable PIM snooping in a VLAN before you execute this command.

Global ports include Layer 2 aggregate interfaces. A global neighbor port is a global port that acts as a neighbor port.

Examples

In VLAN 2, set the aging time to 300 seconds for global neighbor ports on the new master device after a master/subordinate switchover.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] pim-snooping enable
[Sysname-vlan2] pim-snooping graceful-restart neighbor-aging-time 300
```

Related commands

pim-snooping enable

reset pim-snooping statistics

Use **reset pim-snooping statistics** to clear statistics for the PIM messages learned through PIM snooping.

Syntax

reset pim-snooping statistics

Views

User view

Predefined user roles

network-admin

Examples

Clear statistics for the PIM messages learned through PIM snooping.

```
<Sysname> reset pim-snooping statistics
```

Related commands

display pim-snooping statistics

Contents

Multicast VLAN commands

display multicast-vlan

Use **display multicast-vlan** to display information about multicast VLANs.

Syntax

display multicast-vlan [*vlan-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan-id: Specifies a multicast VLAN ID in the range of 1 to 4094. If you do not specify a multicast VLAN ID, this command displays information about all multicast VLANs.

Examples

Display information about all multicast VLANs.

```
<Sysname> display multicast-vlan
Total 2 multicast VLANs.

Multicast VLAN 100:
  Sub-VLAN list(3 in total):
    2-3, 6
  Port list(3 in total):
    GE1/0/1
    GE1/0/2
    GE1/0/3

Multicast VLAN 200:
  Sub-VLAN list(0 in total):
  Port list(0 in total):
```

Table 1 Command output

Field	Description
Total 2 multicast VLANs	Total number of multicast VLANs.
Sub-VLAN list(3 in total)	Sub-VLAN list of the multicast VLAN, and the total number of the sub-VLANs.
Port list(3 in total)	Port list of the multicast VLAN, and the total number of the ports.

display multicast-vlan forwarding-table

Use **display multicast-vlan forwarding-table** to display multicast VLAN forwarding entries.

Syntax

display multicast-vlan forwarding-table [*group-address* [**mask** { *mask-length* | *mask* }] | *source-address* [**mask** { *mask-length* | *mask* }] | **slot** *slot-number* | **subvlan** *vlan-id* | **vlan** *vlan-id*] *

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group-address: Specifies a multicast group by its IP address in the range of 224.0.0.0 to 239.255.255.255. If you do not specify a multicast group, this command displays multicast VLAN forwarding entries for all multicast groups.

mask { *mask-length* | *mask* }: Specifies a mask length or subnet mask for the multicast group address. The value range for the *mask-length* argument is 4 to 32 (default), and the default value for the *mask* argument is 255.255.255.255.

source-address: Specifies a multicast source by its IP address. If you do not specify a multicast source, this command displays multicast VLAN forwarding entries for all multicast sources.

mask { *mask-length* | *mask* }: Specifies a mask length or subnet mask for the multicast source address. The value range for the *mask-length* argument is 0 to 32 (default), and the default value for the *mask* argument is 255.255.255.255.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays multicast VLAN forwarding entries for the master device.

subvlan *vlan-id*: Specifies a sub-VLAN by its VLAN ID. If you do not specify a sub-VLAN, this command displays multicast VLAN forwarding entries for all sub-VLANs.

vlan *vlan-id*: Specifies a multicast VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a multicast VLAN, this command displays multicast VLAN forwarding entries for all multicast VLANs.

Examples

Display all multicast VLAN forwarding entries.

```
<Sysname> display multicast-vlan forwarding-table
Multicast VLAN 100 Forwarding Table
Total 1 entries, 1 matched

00001. (1.1.1.1, 225.0.0.1)
     Flags: 0x10000
     Multicast VLAN: 100
     List of sub-VLANs (3 in total):
       1: VLAN 10
       2: VLAN 20
       3: VLAN 30
```

Table 2 Command output

Field	Description
Multicast VLAN 100 Forwarding Table	Forwarding entries for multicast VLAN 100.
Total 1 entries, 1 matched	Total number of (S, G) entries, and the number of matching entries.
00001	Sequence number of the (S, G) entry.
(1.1.1.1, 255.0.0.1)	(S, G) entry, where **0.0.0.0** in the S position means all multicast sources.
Flags	Entry flag. This field displays one flag or the sum of multiple flags. In this example, the value 0x10000 means that the entry has only one flag 0x10000. The following flags are available for an entry: • **0x1**—The entry is in inactive state. • **0x4**—The entry fails to update. • **0x8**—The sub-VLAN information fails to update for the entry. • **0x200**—The entry is in GR state. • **0x10000**—The entry is a multicast VLAN forwarding entry.
List of sub-VLANs (3 in total)	Sub-VLAN list of the multicast VLAN, and the total number of the sub-VLANs.

display multicast-vlan group

Use **display multicast-vlan group** to display information about multicast groups in multicast VLANs.

Syntax

display multicast-vlan group [*source-address* | *group-address* | **slot** *slot-number* | **verbose** | **vlan** *vlan-id*] *

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

source-address: Specifies a multicast source by its IP address. If you do not specify a multicast source, this command displays information about multicast groups for all multicast sources in multicast VLANs.

group-address: Specifies a multicast group by its IP address in the range of 224.0.1.0 to 239.255.255.255. If you do not specify a multicast group, this command displays information for all multicast groups in multicast VLANs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about multicast groups in multicast VLANs for the master device.

verbose: Displays detailed information.

vlan *vlan-id*: Specifies a multicast VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a multicast VLAN, this command displays information about multicast groups for all multicast VLANs.

Examples

Display detailed information about all multicast groups in multicast VLANs.

```
<Sysname> display multicast-vlan group verbose
Total 6 entries.

Multicast VLAN 10: Total 3 entries.
  (2.2.2.2, 225.1.1.2)
    Flags: 0x70000020
    Sub-VLANs (1 in total):
      VLAN 40
  (111.112.113.115, 225.1.1.4)
    Flags: 0x70000030
    Sub-VLANs (1 in total):
      VLAN 40
  (0.0.0.0, 226.1.1.6)
    Flags: 0x60000020
    Sub-VLANs (1 in total):
      VLAN 40

Multicast VLAN 20: Total 3 entries.
  (2.2.2.2, 225.1.1.2)
    Flags: 0x70000010
    Sub-VLANs (0 in total):
  (111.112.113.115, 225.1.1.4)
    Flags: 0x70000010
    Sub-VLANs (0 in total):
  (0.0.0.0, 226.1.1.6)
    Flags: 0x50000010
    Sub-VLANs (0 in total):
```

Table 3 Command output

Field	Description
Total 6 entries	Total number of (S, G) entries.
Multicast VLAN 10: Total 3 entries	Total number of (S, G) entries in multicast VLAN 10.
(0.0.0.0, 226.1.1.6)	(S, G) entry, where **0.0.0.0** in the S position means all multicast sources.
Flags	Entry flag. This field displays one flag or the sum of multiple flags. For example, the value 0x70000020 means that the entry has flags 0x20, 0x10000000, 0x20000000, and 0x40000000. The following flags are available for an entry: • **0x10**—The entry is created by the multicast VLAN. • **0x20**—The entry is created by the sub-VLAN of the multicast VLAN. • **0x40**—The entry is to be deleted.

Field	Description

	• **0x10000000**—This value represents one of the following situations:
	  ◦ The entry is newly created.
	  ◦ The device receives an IGMP query that matches the (S, G) entry but does not receive any matching IGMPv1 reports within an IGMP general query interval.
	• **0x20000000**—The device does not receive IGMPv2 or IGMPv3 reports that match the (S, G) entry within an IGMP general query interval.
	• **0x40000000**—The device does not receive IGMPv3 IS_EX (NULL) reports that match the (S, G) entry within an IGMP general query interval.

Sub-VLANs (1 in total)	Sub-VLAN list of the multicast VLAN, and the total number of the sub-VLANs.

Related commands

reset multicast-vlan group

multicast-vlan

Use **multicast-vlan** to configure a multicast VLAN and enter its view, or enter the view of an existing multicast VLAN.

Use **undo multicast-vlan** to remove the configuration of multicast VLANs.

Syntax

multicast-vlan *vlan-id*

undo multicast-vlan { **all** | *vlan-id* }

Default

No multicast VLANs exist.

Views

System view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies an existing VLAN by its ID in the range of 1 to 4094.

all: Specifies all multicast VLANs.

Usage guidelines

You can configure a maximum of five multicast VLANs.

You must enable IGMP snooping for the VLAN to be configured as a multicast VLAN.

Examples

Enable IGMP snooping for VLAN 100. Configure VLAN 100 as a multicast VLAN and enter its view.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 100
```

```
[Sysname-vlan100] igmp-snooping enable
[Sysname-vlan100] quit
[Sysname] multicast-vlan 100
[Sysname-mvlan-100]
```

Related commands

`igmp-snooping enable`

multicast-vlan entry-limit

Use **`multicast-vlan entry-limit`** to set the maximum number of multicast VLAN forwarding entries.

Use **`undo multicast-vlan entry-limit`** to restore the default.

Syntax

`multicast-vlan entry-limit` *`limit`*

`undo multicast-vlan entry-limit`

Default

The following matrix shows the default values for the maximum number of multicast VLAN forwarding entries:

Hardware	Maximum number of multicast VLAN forwarding entries
S5110V2-SI switch series S5000V3-EI switch series S5000V5-EI switch series S5000E-X switch series S5000X-EI switch series S5110V2 switch series WS5810-WiNet switch series	240
S5120V2-LI switch series S5130S-LI switch series S5120V3-SI switch series MS4320V2 switch series MS4320 switch series	500
WAS6000 switch series	• WAS6124 and WAS6148: 500 • Other switches: 240
S3100V3-SI switch series	• Switches with product code LS-3100V3-18TP-SI-H1, LS-3100V3-28TP-SI-H1, LS-3100V3-52TP-SI-H1, or LS-3100V3-20TP-PWR-SI-H1: 240 • Other switches: 500
MS4200 switch series	• Switches with product code LS-MS4200-28TP-H1, LS-MS4200-18TP-H1, or LS-MS4200-20TP-PWR-H1: 240 • Other switches: 500

WS5820-WiNet switch series	• Switches with product code WS5820-28P-POE-WiNet: 240 • Other switches: 500
MS4300V2 switch series	• MS4300V2-28P, MS4300V2-52P: 240 • MS4300V2-10P: 500
MS4320V3 switch series	• MS4320V3-28P, MS4320V3-52P: 240 • Other switches: 500
S5120V3-LI switch series	• S5120V2-20P-LI, S5120V2-28P-LI, S5120V2-52P-LI, S5120V2-28P-PWR-LI, S5120V2-52P-PWR-LI: 240 • Other switches: 500

Views

System view

Predefined user roles

network-admin

Parameters

limit: Specifies the maximum number of multicast VLAN forwarding entries. The following matrix shows the value range for this argument:

Hardware	Value range
S5110V2-SI switch series S5000V3-EI switch series S5000V5-EI switch series S5000E-X switch series S5000X-EI switch series WAS6000 switch series S5110V2 switch series WS5810-WiNet switch series	0 to 240
S5120V2-LI switch series S5130S-LI switch series S5120V3-SI switch series MS4320V2 switch series MS4320 switch series	0 to 500
S3100V3-SI switch series	• Switches with product code LS-3100V3-18TP-SI-H1, LS-3100V3-28TP-SI-H1, LS-3100V3-52TP-SI-H1, or LS-3100V3-20TP-PWR-SI-H1: 0 to 240 • Other switches: 0 to 500
MS4200 switch series	• Switches with product code LS-MS4200-28TP-H1, LS-MS4200-18TP-H1, or LS-MS4200-20TP-PWR-H1: 0 to 240 • Other switches: 0 to 500
WS5820-WiNet switch series	• Switches with product code WS5820-28P-POE-WiNet: 0 to 240 • Other switches: 0 to 500

MS4300V2 switch series	• MS4300V2-28P, MS4300V2-52P: 0 to 240 • MS4300V2-10P: 0 to 500
MS4320V3 switch series	• MS4320V3-28P, MS4320V3-52P: 0 to 240 • Other switches: 0 to 500
S5120V3-LI switch series	• S5120V2-20P-LI, S5120V2-28P-LI, S5120V2-52P-LI, S5120V2-28P-PWR-LI, S5120V2-52P-PWR-LI: 0 to 240 • Other switches: 0 to 500

Usage guidelines

If the configured value is smaller than the current number of multicast VLAN forwarding entries, the device cannot create new entries until some entries age out or are manually removed. To allow new entries to be created immediately, use the **reset multicast-vlan group** command to remove multicast VLAN forwarding entries.

Examples

Set the maximum number of multicast VLAN forwarding entries to 128.

```
<Sysname> system-view
[Sysname] multicast-vlan entry-limit 128
```

Related commands

entry-limit (IGMP-snooping view)

port (multicast-VLAN view)

Use **port** to assign user ports to a multicast VLAN.

Use **undo port** to delete user ports from a multicast VLAN.

Syntax

port *interface-list*

undo port { **all** | *interface-list* }

Default

A multicast VLAN does not have user ports.

Views

Multicast VLAN view

Predefined user roles

network-admin

Parameters

interface-list: Specifies a port in the form of *interface-type interface-number*, or a port range in the form of *interface-type interface-number* to *interface-type interface-number*.

all: Specifies all user ports in the current multicast VLAN.

Usage guidelines

You can assign only Layer 2 Ethernet ports or Layer 2 aggregate interfaces to multicast VLANs. Additionally, you can assign a port to only one multicast VLAN.

For ports to be assigned to a multicast VLAN, you must enable IGMP snooping for the VLANs to which the ports belong.

Examples

Assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 as user ports to multicast VLAN 100.

```
<Sysname> system-view
[Sysname] multicast-vlan 100
[Sysname-mvlan-100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

port multicast-vlan

Use **port multicast-vlan** to assign a user port to a multicast VLAN.

Use **undo port multicast-vlan** to restore the default.

Syntax

port multicast-vlan *vlan-id*

undo port multicast-vlan

Default

A port does not belong to a multicast VLAN.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies a multicast VLAN by its VLAN ID in the range of 1 to 4094.

Usage guidelines

You can assign a port to only one multicast VLAN.

For a port to be assigned to a multicast VLAN, you must enable IGMP snooping for the VLAN to which the port belongs.

Examples

Assign GigabitEthernet 1/0/1 as a user port to multicast VLAN 100.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port multicast-vlan 100
```

reset multicast-vlan group

Use **reset multicast-vlan group** to clear multicast groups in multicast VLANs.

Syntax

reset multicast-vlan group [*source-address* [**mask** { *mask-length* | *mask* }] | *group-address* [**mask** { *mask-length* | *mask* }] | **vlan** *vlan-id*] *

Views

User view

Predefined user roles

network-admin

Parameters

source-address: Specifies a multicast source by its IP address. If you do not specify a multicast source, this command clears multicast groups for all multicast sources in multicast VLANs.

mask { *mask-length* | *mask* }: Specifies a mask length or subnet mask for the multicast source address. The value range for the *mask-length* argument is 0 to 32 (default), and the default value for the *mask* argument is 255.255.255.255.

group-address: Specifies a multicast group by its IP address in the range of 224.0.1.0 to 239.255.255.255. If you do not specify a multicast group, this command clears all multicast groups in multicast VLANs.

mask { *mask-length* | *mask* }: Specifies a mask length or subnet mask for the multicast group address. The value range for the *mask-length* argument is 4 to 32 (default), and the default value for the *mask* argument is 255.255.255.255.

vlan *vlan-id*: Specifies a multicast VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a multicast VLAN, this command clears multicast groups for all multicast VLANs.

Examples

Clear multicast groups for all multicast VLANs.

```
<Sysname> reset multicast-vlan group
```

Related commands

display multicast-vlan group

subvlan (multicast-VLAN view)

Use **subvlan** to assign VLANs as sub-VLANs to a multicast VLAN.

Use **undo subvlan** to delete sub-VLANs from a multicast VLAN.

Syntax

subvlan *vlan-list*

undo subvlan { **all** | *vlan-list* }

Default

A multicast VLAN does not have sub-VLANs.

Views

Multicast VLAN view

Predefined user roles

network-admin

Parameters

vlan-list: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The value range for the VLAN ID is 1 to 4094. The specified VLANs must exist and cannot be multicast VLANs or sub-VLANs of other multicast VLANs.

all: Specifies all sub-VLANs of the current multicast VLAN.

Usage guidelines

You must enable IGMP snooping for VLANs to be configured as sub-VLANs.

Examples

Assign VLAN 10 through VLAN 15 as sub-VLANs to multicast VLAN 100.

```
<Sysname> system-view
[Sysname] multicast-vlan 100
[Sysname-mvlan-100] subvlan 10 to 15
```

Contents

MLD snooping commands

display ipv6 l2-multicast fast-forwarding cache

Use **display ipv6 l2-multicast fast-forwarding cache** to display Layer 2 IPv6 multicast fast forwarding entries.

Syntax

display ipv6 l2-multicast fast-forwarding cache [**vlan** *vlan-id*] [*ipv6-source-address* | *ipv6-group-address*] * [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

ipv6-source-address: Specifies an IPv6 multicast source address. If you do not specify an IPv6 multicast source, this command displays Layer 2 IPv6 multicast forwarding entries for all IPv6 multicast sources.

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F. If you do not specify an IPv6 multicast group, this command displays Layer 2 IPv6 multicast forwarding entries for all IPv6 multicast groups.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays Layer 2 IPv6 multicast fast forwarding entries for the master device.

Examples

Display Layer 2 IPv6 multicast fast forwarding entries.

```
<Sysname> display ipv6 l2-multicast fast-forwarding cache
Total 1 entries, 1 matched

(1::6, FF1E::2)
      Status      : Enable                VLAN            : 1
      Source port : 9876                  Destination port: 5432
      Protocol    : 17                    Flag            : 0x2
      Ingress port: GigabitEthernet1/0/2
      List of 1 egress ports:
           GigabitEthernet1/0/3
           Status: Enable                Flag: 0x10
```

Table 1 Command output

Field	Description
Total 1 entries, 1 matched	Total number of (S, G) entries in the Layer 2 IPv6 multicast fast forwarding table, and the total number of matching entries.

Field	Description
(1::6, FF1E::2)	(S, G) entry in the Layer 2 IPv6 multicast fast forwarding table.
Protocol	Protocol number.
VLAN	VLAN ID.
Flag	Flag for the (S, G) entry or the outgoing port. This field displays one flag or the sum of multiple flags. In this example, the value 0x2 means that the entry has only one flag 0x2. The following flags are available for an entry: • **0x1**—The entry is created because of packets passed through between cards. • **0x2**—The entry is added by multicast forwarding. The following flags are available for an outgoing interface: • **0x1**—The port is added to the entry because of packets passed through between cards. • **0x2**—The port is added to an existing entry. • **0x10**—The port is associated with the entry. • **0x20**—The port is to be deleted.
Status	Status of the (S, G) entry or the outgoing port: • **Enabled**—Available. • **Disabled**—Unavailable.
Ingress port	Incoming port of the (S, G) entry.
List of 1 egress ports	List of outgoing ports of the (S, G) entry.

Related commands

`reset ipv6 l2-multicast fast-forwarding cache all`

display ipv6 l2-multicast ip

Use **`display ipv6 l2-multicast ip`** to display information about Layer 2 IPv6 multicast groups.

Syntax

`display ipv6 l2-multicast ip` [**`group`** *`ipv6-group-address`* | **`source`** *`ipv6-source-address`*] * [**`vlan`** *`vlan-id`*] [**`slot`** *`slot-number`*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

`group` *`ipv6-group-address`*: Specifies an IPv6 multicast group by its IPv6 address. If you do not specify an IPv6 multicast group, this command displays information about all Layer 2 IPv6 multicast groups.

`source` *`ipv6-source-address`*: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, this command displays information about Layer 2 IPv6 multicast groups for all IPv6 multicast sources.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays information about Layer 2 IPv6 multicast groups for all VLANs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about Layer 2 IP multicast groups for the master device.

Examples

Display information about Layer 2 IPv6 multicast groups for VLAN 2.

```
<Sysname> display ipv6 l2-multicast ip vlan 2
Total 1 entries.

VLAN 2: Total 1 entries.
   (::, FF1E::101)
    Attribute: static, success
    Host ports (1 in total):
      GE1/0/1                                (S, SUC)
```

Table 2 Command output

Field	Description
Total 1 entries	Total number of Layer 2 IPv6 multicast groups.
VLAN 2: Total 1 entries	Total number of Layer 2 IPv6 multicast groups in VLAN 2.
(::, FF1E::101)	(S, G) entry, where a double colon (::) in the S position means all IPv6 multicast sources.
Attribute	Entry attribute: • **dynamic**—The entry is created by a dynamic protocol. • **static**—The entry is created by a static protocol. • **pim**—The entry is created by IPv6 PIM. • **kernel**—The entry is obtained from the kernel. • **success**—Processing has succeeded. • **fail**—Processing has failed.
Host ports (1 in total)	Member ports and total number of member ports.
(S, SUC)	Port attribute: • **D**—Dynamic port. • **S**—Static port. • **P**—IPv6 PIM port. • **K**—Port obtained from the kernel. • **R**—Port learned from (*, *) entries. • **W**—Port learned from (*, G) entries. • **SUC**—Processing has succeeded. • **F**—Processing has failed.

display ipv6 l2-multicast ip forwarding

Use **display ipv6 l2-multicast ip forwarding** to display Layer 2 IPv6 multicast IP forwarding entries.

Syntax

display ipv6 l2-multicast ip forwarding [**group** *ipv6-group-address* | **source** *ipv6-source-address*] * [**vlan** *vlan-id*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group *ipv6-group-address*: Specifies an IPv6 multicast group by its IPv6 address. If you do not specify an IPv6 multicast group, this command displays Layer 2 IPv6 multicast IP forwarding entries for all IPv6 multicast groups.

source *ipv6-source-address*: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, this command displays Layer 2 IPv6 multicast IP forwarding entries for all IPv6 multicast sources.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays Layer 2 IPv6 multicast IP forwarding entries for all VLANs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays Layer 2 IPv6 multicast IP forwarding entries for the master device.

Examples

Display Layer 2 IPv6 multicast IP forwarding entries for VLAN 2.

```
<Sysname> display ipv6 l2-multicast ip forwarding vlan 2
Total 1 entries.

VLAN 2: Total 1 entries.
   (::, FF1E::101)
    Host ports (3 in total):
      GigabitEthernet1/0/1
      GigabitEthernet1/0/2
      GigabitEthernet1/0/3
```

Table 3 Command output

Field	Description
Total 1 entries	Total number of Layer 2 IPv6 multicast IP forwarding entries.
VLAN 2: Total 1 entries	Total number of Layer 2 IPv6 multicast IP forwarding entries in VLAN 2.
(::, FF1E::101)	(S, G) entry, where a double colon (::) in the S position means all IPv6 multicast sources.
Host ports (3 in total)	Member ports and total number of member ports.

display ipv6 l2-multicast mac

Use **display ipv6 l2-multicast mac** to display information about Layer 2 IPv6 multicast MAC multicast groups.

Syntax

display ipv6 l2-multicast mac [*mac-address*] [**vlan** *vlan-id*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

mac-address: Specifies an IPv6 multicast MAC address. If you do not specify an IPv6 multicast MAC address, this command displays information about all Layer 2 IPv6 multicast MAC multicast groups.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays information about Layer 2 IPv6 multicast MAC multicast groups for all VLANs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about Layer 2 IPv6 multicast MAC multicast groups for the master device.

Examples

Display information about Layer 2 IPv6 multicast MAC multicast groups for VLAN 2.

```
<Sysname> display ipv6 l2-multicast mac vlan 2
Total 1 entries.

VLAN 2: Total 1 entries.
  MAC group address: 3333-0000-0101
    Attribute: success
    Host ports (1 in total):
      GE1/0/1
```

Table 4 Command output

Field	Description
Total 1 entries	Total number of Layer 2 IPv6 MAC multicast groups.
VLAN 2: Total 1 entries	Total number of Layer 2 IPv6 MAC multicast groups in VLAN 2.
MAC group address	IPv6 address of the Layer 2 IPv6 MAC multicast group.
Attribute	Entry attribute: • **success**—Processing has succeeded. • **fail**—Processing has failed.
Host ports (1 in total)	Member ports and total number of member ports.

display ipv6 l2-multicast mac forwarding

Use **display ipv6 l2-multicast mac forwarding** to display Layer 2 IPv6 multicast MAC forwarding entries.

Syntax

display ipv6 l2-multicast mac forwarding [*mac-address*] [**vlan** *vlan-id*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

mac-address: Specifies an IPv6 MAC multicast group by its IPv6 MAC address. If you do not specify an IPv6 MAC multicast group, this command displays Layer 2 IPv6 multicast MAC forwarding entries for all IPv6 MAC multicast groups.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays Layer 2 IPv6 multicast MAC forwarding entries for all VLANs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays Layer 2 IPv6 multicast MAC forwarding entries for the master device.

Examples

Display Layer 2 IPv6 multicast MAC forwarding entries for VLAN 2.

```
<Sysname> display ipv6 l2-multicast mac forwarding vlan 2
Total 1 entries.

VLAN 2: Total 1 entries.
  MAC group address: 3333-0000-0101
    Host ports (3 in total):
      GigabitEthernet1/0/1
      GigabitEthernet1/0/2
      GigabitEthernet1/0/3
```

Table 5 Command output

Field	Description
Total 1 MAC entries	Total number of Layer 2 IPv6 multicast MAC forwarding entries.
VLAN 2: Total 1 entries	Total number of Layer 2 IPv6 multicast MAC forwarding entries in VLAN 2.
MAC group address	Address of the IPv6 MAC multicast group.
Host ports (3 in total)	Member ports, and the total number of member ports.

display mld-snooping

Use **display mld-snooping** to display MLD snooping status.

Syntax

display mld-snooping [**global** | **vlan** *vlan-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

`global`: Displays the global MLD snooping status.

`vlan` *`vlan-id`*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

Usage guidelines

If you do not specify any parameters, this command displays the global MLD snooping status and the MLD snooping status in all VLANs.

Examples

Display the global MLD snooping status and the MLD snooping status for all VLANs.

```
<Sysname> display mld-snooping
MLD snooping information: Global
  Global-enable: Enabled
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-listener-query-interval: 1s
 Report-aggregation: Enabled
 Host-tracking: Disabled
 Dot1p-priority: --

MLD snooping information: VLAN 1
 MLD snooping: Enabled
 Drop-unknown: Disabled
 Version: 1
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-listener-query-interval: 1s
 Querier: Enabled (IP: FE80::2FF:FFFF:FE00:1, Expires: 00:02:05)
 Querier-election: Enabled
 Query-interval: 125s
 General-query source IP: FE80::2FF:FFFF:FE00:1
 Special-query source IP: FE80::2FF:FFFF:FE00:1
 Report source IP: FE80::2FF:FFFF:FE00:2
 Done source IP: FE80::2FF:FFFF:FE00:3
 Host-tracking: Disabled
 Dot1p-priority: 2
 Proxy: Disabled

MLD snooping information: VLAN 10
 MLD snooping: Enabled
 Drop-unknown: Enabled
 Version: 1
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-listener-query-interval: 1s
```

```
Querier: Enabled (IP: FE80::2FF:FFFF:FE00:1, Expires: 00:02:05)
Querier-election: Enabled
Query-interval: 125s
General-query source IP: FE80::2FF:FFFF:FE00:1
Special-query source IP: FE80::2FF:FFFF:FE00:1
Report source IP: FE80::2FF:FFFF:FE00:2
Done source IP: FE80::2FF:FFFF:FE00:3
Host-tracking: Disabled
Dot1p-priority: --
Proxy: Disabled
```

Table 6 Command output

Field	Description
Global-enable	Global MLD snooping status: • Enabled. • Disabled.
MLD snooping	MLD snooping status in a VLAN: • **Enabled**. • **Disabled**. • **Globally enabled**. • **Inactive**—MLD snooping configuration does not take effect.
Drop-unknown	Status of dropping unknown IPv6 multicast data: • Enabled. • Disabled.
Version	MLD snooping version.
Host-aging-time	Aging timer for the dynamic member port.
Router-aging-time	Aging timer for the dynamic router port.
Max-response-time	Maximum time for responding to MLD general queries.
Last-listener-query-interval	Interval for sending MLD multicast-address-specific queries.
Report-aggregation	Status of MLD report suppression: • Enabled. • Disabled.
Dot1p-priority	802.1p priority for MLD messages. This field displays two hyphens (--) if the 802.1p priority is not configured.
Querier	Status of MLD snooping querier: • Enabled. • Disabled.
(IP: FE80::2FF:FFFF:FE00:1, Expires: 00:02:05)	MLD snooping querier information: • **IP**—IP address of the MLD snooping querier. • **Expire**—Remaining aging time for the MLD snooping querier. This field is not displayed if MLD snooping querier election is disabled.
Querier-election	Status of MLD snooping querier election: • Enabled. • Disabled.
Query-interval	Interval for sending MLD general queries.

Field	Description
General-query source IP	Source IPv6 address of MLD general queries.
Special-query source IP	Source IPv6 address of MLD multicast-address-specific queries.
Report source IP	Source IPv6 address of MLD reports.
Done source IP	Source IPv6 address of MLD done messages.
Host-tracking	Status of host tracking: • Enabled. • Disabled. • Globally enabled.
Proxy	Status of MLD snooping proxying: • Enabled. • Disabled.

display mld-snooping group

Use **display mld-snooping group** to display information about dynamic MLD snooping group entries.

Syntax

display mld-snooping group [*ipv6-group-address* | *ipv6-source-address*] * [**vlan** *vlan-id*] [**interface** *interface-type interface-number* | [**verbose**] [**slot** *slot-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F. If you do not specify an IPv6 multicast group, this command displays information about all dynamic MLD snooping group entries.

ipv6-source-address: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, this command displays information about dynamic MLD snooping group entries for all IPv6 multicast sources.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays information about dynamic MLD snooping group entries for all VLANs.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays brief information about dynamic MLD snooping group entries for all interfaces.

verbose: Displays detailed information about dynamic MLD snooping group entries. If you do not specify this keyword, the command displays brief information about dynamic MLD snooping group entries.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about dynamic MLD snooping group entries for the master device.

Examples

Display brief information about dynamic MLD snooping group entries for GigabitEthernet 1/0/1.

```
<Sysname> display mld-snooping group interface
Total 1 entries.

GE1/0/1:
  VLAN 2: Total 1 entries.
   (::,FF1E::101)                    (00:03:23)
```

Display detailed information about dynamic MLD snooping group entries for VLAN 2.

```
<Sysname> display mld-snooping group vlan 2 verbose
Total 2 entries.

VLAN 2: Total 2 entries.
  (::,FF1E::101)
    Attribute: local port
    FSM information: dummy
    Host slots (0 in total):
    Host ports (1 in total):
      GE1/0/2                              (00:03:23)
  (12::, FF1E::101)
    Attribute: local port
    FSM information: dummy
    Host ports (1 in total):
      GE1/0/2                             (00:04:02)
```

Table 7 Command output

Field	Description
Total 1 entries	Total number of dynamic MLD snooping group entries.
VLAN 2: Total 1 entries	Total number of dynamic MLD snooping group entries in VLAN 2.
(::, FF1E::101)	(S, G) entry, where a double colon (::) in the S position means all IPv6 multicast sources.
Attribute	Entry attribute: • **global port**—The entry has a global port. • **local port**—The entry has a port that resides on the member device for which the information is displayed. • **slot**—The entry has ports that reside on other member devices, but not on the member device for which the information is displayed.
FSM information	Finite state machine information of the entry: • **delete**—The entry attributes have been deleted. • **dummy**—The entry is a new temporary entry. • **no info**—The entry does not exist. • **normal**—The entry is a correct entry.
Host slots (0 in total)	Member IDs and total number of the member devices that have member ports, except for the specified member device or the master device when no member device is specified.

Field	Description
Host ports (1 in total)	Member ports and total number of member ports.
(00:03:23)	Remaining aging time for the dynamic member port. This field is always displayed for a global port (such as Layer 2 aggregate interfaces). For a non-global port, this field is displayed when one of the following conditions exists: • The port is on the specified member device. • The port is on the master device and no member device is specified.

Related commands

reset mld-snooping group

display mld-snooping host-tracking

Use **display mld-snooping host-tracking** to display host tracking information.

Syntax

display mld-snooping host-tracking vlan *vlan-id* **group** *ipv6-group-address* [**source** *ipv6-source-address*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

group *ipv6-group-address*: Specifies an IPv6 multicast group by its IPv6 address. The value range for the *ipv6-group-address* argument is FFxy::/16, where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

source *ipv6-source-address*: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, this commands displays host tracking information for all IPv6 multicast sources.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays host tracking information for the master device.

Examples

Display tracking information for hosts that have joined IPv6 multicast group FF1E::2 in VLAN 2.

```
<Sysname> display mld-snooping host-tracking vlan 2 group FF1E::2
VLAN 2
 (1::6, FF1E::2)
    Port: GE1/0/1
      Host                                    Uptime          Expires
      1::2                                    00:02:20        00:00:40
      1::3                                    00:02:21        00:00:39
```

Table 8 Command output

Field	Description
VLAN	VLAN ID.
(1::6, FF1E::2)	(S, G) entry, where 0::0 in the S position means any IPv6 multicast sources.
Port	Member port.
Host	IPv6 address of the host.
Uptime	Length of time elapsed since the host joined the IPv6 multicast group.
Expires	Remaining timeout time for the host. The host timeout time is the same as the aging timer of the port. The timer is reset when the port receives an MLD report from the host. This field displays **timeout** if the host times out.

Related commands

host-tracking (MLD-snooping view)

mld-snooping enable

mld-snooping host-tracking

display mld-snooping router-port

Use **display mld-snooping router-port** to display dynamic router port information.

Syntax

display mld-snooping router-port [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

verbose: Displays detailed information about dynamic router ports. If you do not specify this keyword, the command displays brief information about dynamic router ports.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays dynamic router port information for all VLANs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays dynamic router port information for the master device.

Examples

Display brief information about dynamic router ports for VLAN 2.

```
<Sysname> display mld-snooping router-port vlan 2
VLAN 2:
  Router ports (2 in total):
    GE1/0/1                          (00:01:30)
    GE1/0/2                          (00:00:23)
```

Display detailed information about dynamic router ports for VLAN 2.

```
<Sysname> display mld-snooping router-port vlan 2 verbose
VLAN 2:
  Router slots (0 in total):
  Router ports (2 in total):
    GE1/0/1                          (00:01:30)
    GE1/0/2                          (00:00:23)
```

Table 9 Command output

Field	Description
VLAN 2	VLAN ID.
Router slots (0 in total)	Member IDs and total number of the member devices that have dynamic router ports, except for the specified member device or the master device when no member device is specified.
Router ports (2 in total)	Dynamic router ports and total number of dynamic router ports.
(00:01:30)	Remaining aging time for the dynamic router port. This field is always displayed for a global port (including Layer 2 aggregate interfaces). For a non-global port, this field is displayed when one of the following conditions exists: • The port is on the specified member device. • The port is on the master device and no member device is specified.

Related commands

reset mld-snooping router-port

display mld-snooping static-group

Use **display mld-snooping static-group** to display information about static MLD snooping group entries.

Syntax

display mld-snooping static-group [*ipv6-group-address* | *ipv6-source-address*] * [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6-group-address: Specifies an IPv6 multicast group by its IPv6 address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F. If you do not specify an IPv6 multicast group, this command displays information about static MLD snooping group entries for all IPv6 multicast groups.

ipv6-source-address: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, this command displays information about static MLD snooping group entries for all IPv6 multicast sources.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays information about static MLD snooping group entries for all VLANs.

verbose: Displays detailed information. If you do not specify this keyword, the command displays brief information.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about static MLD snooping group entries for the master device.

Examples

Display detailed information about static MLD snooping group entries for VLAN 2.

```
<Sysname> display mld-snooping static-group vlan 2 verbose
Total 1 entries.

VLAN 2: Total 1 entries.
  (::,FF1E::101)
    Attribute: local port
    FSM information: dummy
    Host slots (0 in total):
    Host ports (1 in total):
      GE1/0/2
```

Table 10 Command output

Field	Description
Total 1 entries	Total number of static MLD snooping group entries.
VLAN 2: Total 1 entries	Total number of static MLD snooping group entries in VLAN 2.
(::, FF1E::101)	(S, G) entry, where a double colon (::) in the S position means all IPv6 multicast sources.
Attribute	Entry attribute: • **global port**—The entry has a global port. • **local port**—The entry has a port that resides on the member device for which the information is displayed. • **slot**—The entry has ports that reside on other member devices, but not on the member device for which the information is displayed.
FSM information	Finite state machine information of the entry: • **delete**—The entry attributes have been deleted. • **dummy**—The entry is a new temporary entry. • **no info**—The entry does not exist. • **normal**—The entry is a correct entry.
Host slots (0 in total)	Member IDs and total number of the member devices that have member ports, except for the specified member device or the master device when no member device is specified.
Host ports (1 in total)	Member ports and total number of member ports.

display mld-snooping static-router-port

Use **display mld-snooping static-router-port** to display static router port information.

Syntax

display mld-snooping static-router-port [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

verbose: Displays detailed information about static router ports. If you do not specify this keyword, the command displays brief information about static router ports.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays static router port information for the master device.

Examples

Display brief information about static router ports for VLAN 2.

```
<Sysname> display mld-snooping static-router-port vlan 2
VLAN 2:
  Router ports (2 in total):
    GE1/0/1
    GE1/0/2
```

Display detailed information about static router ports for VLAN 2.

```
<Sysname> display mld-snooping static-router-port vlan 2 verbose
VLAN 2:
  Router slots (0 in total):
  Router ports (2 in total):
    GE1/0/1
    GE1/0/2
```

Table 11 Command output

Field	Description
VLAN 2	VLAN ID.
Router slots (0 in total)	Member IDs and total number of the member devices that have static router ports, except for the specified member device or the master device when no member device is specified.
Router ports (2 in total)	Static router ports and total number of static router ports.

display mld-snooping statistics

Use **display mld-snooping statistics** to display statistics for the MLD messages and IPv6 PIM hello messages learned through MLD snooping.

Syntax

display mld-snooping statistics

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display statistics for the MLD messages and IPv6 PIM hello messages learned through MLD snooping.

```
<Sysname> display mld-snooping statistics
Received MLD general queries:  0
Received MLDv1 specific queries:  0
Received MLDv1 reports:  0
Received MLD dones:  0
Sent     MLDv1 specific queries:  0
Received MLDv2 reports:  0
Received MLDv2 reports with right and wrong records:  0
Received MLDv2 specific queries:  0
Received MLDv2 specific sg queries:  0
Sent     MLDv2 specific queries:  0
Sent     MLDv2 specific sg queries:  0
Received IPv6 PIM hello:  0
Received error MLD messages:  0
```

Table 12 Command output

Field	Description
general queries	Number of MLD general queries.
specific queries	Number of MLD multicast-address-specific queries.
reports	Number of MLD reports.
dones	Number of MLD done messages.
reports with right and wrong records	Number of MLD reports with correct and incorrect records.
specific sg queries	Number of MLD multicast-address-and-source-specific queries.
IPv6 PIM hello	Number of IPv6 PIM hello messages.
error MLD messages	Number of MLD messages with errors.

Related commands

`reset mld-snooping statistics`

dot1p-priority (MLD-snooping view)

Use **`dot1p-priority`** to set the 802.1p priority for MLD messages globally.

Use **`undo dot1p-priority`** to restore the default.

Syntax

`dot1p-priority` *`priority`*

undo dot1p-priority

Default

The global 802.1p priority for MLD messages is 6.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

priority: Specifies an 802.1p priority for MLD messages, in the range of 0 to 7. The greater the value, the higher the priority.

Usage guidelines

You can set the 802.1p priority globally for all VLANs in MLD-snooping view or for a VLAN in VLAN view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

Examples

Set the 802.1p priority for MLD messages to 3 globally.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] dot1p-priority 3
```

Related commands

mld-snooping dot1p-priority

dscp

Use **dscp** to set the DSCP value for outgoing MLD protocol packets.

Use **undo dscp** to restore the default.

Syntax

dscp *dscp-value*

undo dscp

Default

The DSCP value is 48 for outgoing MLD protocol packets.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63.

Usage guidelines

The DSCP value is carried in the Traffic Class field of an IPv6 packet to determine the transmission priority of the packet. A greater DSCP value represents a higher priority.

Examples

Set the DSCP value to 63 for outgoing MLD protocol packets.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] dscp 63
```

enable (MLD-snooping view)

Use **enable** to enable MLD snooping for VLANs.

Use **undo enable** to disable MLD snooping for VLANs.

Syntax

enable vlan *vlan-list*

undo enable vlan *vlan-list*

Default

The MLD snooping status in a VLAN is consistent with the global MLD snooping status.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094.

Usage guidelines

You must enable the MLD snooping feature by using the **mld-snooping** command before you enable MLD snooping for VLANs.

You can enable MLD snooping for multiple VLANs by using this command in MLD-snooping view or for a VLAN by using the **mld-snooping enable** command in VLAN view. The configuration in VLAN view has the same priority as the configuration in MLD-snooping view, and the most recent configuration takes effect.

Examples

Enable the MLD snooping feature, and then enable MLD snooping for VLAN 2 through VLAN 10.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] enable vlan 2 to 10
```

Related commands

mld-snooping

mld-snooping enable

entry-limit (MLD-snooping view)

Use **entry-limit** to globally set the maximum number of MLD snooping forwarding entries, including dynamic entries and static entries.

Use **undo entry-limit** to restore the default.

Syntax

entry-limit *limit*

undo entry-limit

Default

The maximum number of MLD snooping forwarding entries is 4294967295.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

limit: Specifies the maximum number of MLD snooping forwarding entries, in the range of 0 to 4294967295.

Examples

Set the global maximum number of MLD snooping forwarding entries to 512.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] entry-limit 512
```

fast-leave (MLD-snooping view)

Use **fast-leave** to enable fast-leave processing globally.

Use **undo fast-leave** to disable fast-leave processing globally.

Syntax

fast-leave [**vlan** *vlan-list*]

undo fast-leave [**vlan** *vlan-list*]

Default

Fast-leave processing is disabled.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect for all VLANs.

Usage guidelines

The fast-leave processing feature enables the device to immediately remove a port from the forwarding entry for an IPv6 multicast group when the port receives a done message.

You can enable fast-leave processing globally for all ports in MLD-snooping view or for a port in interface view. For a port, the port-specific configuration takes priority over the global configuration.

Examples

Globally enable MLD snooping fast-leave processing for VLAN 2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] fast-leave vlan 2
```

Related commands

mld-snooping fast-leave

global-enable (MLD-snooping view)

Use **global-enable** to enable MLD snooping globally.

Use **undo global-enable** to disable MLD snooping globally.

Syntax

global-enable

undo global-enable

Default

MLD snooping is disabled globally.

Views

MLD-snooping view

Predefined user roles

network-admin

Usage guidelines

To configure other MLD snooping features for VLANs, you must enable MLD snooping for the specific VLANs even though MLD snooping is enabled globally.

Examples

Enable MLD snooping globally.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] global-enable
```

Related commands

enable (MLD-snooping view)

mld-snooping

mld-snooping disable

mld-snooping enable

group-policy (MLD-snooping view)

Use **group-policy** to globally configure an IPv6 multicast group policy to control the IPv6 multicast groups that hosts can join.

Use **undo group-policy** to globally delete IPv6 multicast group policies.

Syntax

group-policy *ipv6-acl-number* [**vlan** *vlan-list*]

undo group-policy [**vlan** *vlan-list*]

Default

No IPv6 multicast group policies exist. Hosts can join any IPv6 multicast groups.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies an IPv6 basic or advanced ACL by its number in the range of 2000 to 3999. Hosts can join only IPv6 multicast groups that the ACL permits. If the ACL does not exist or does not have valid rules, hosts cannot join IPv6 multicast groups.

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect for all VLANs.

Usage guidelines

An IPv6 multicast group policy filters MLD reports to control the IPv6 multicast groups that hosts can join.

This command does not take effect on static member ports, because static member ports do not send MLD reports.

You can configure an IPv6 multicast group policy globally for all ports in MLD-snooping view or for a port in interface view. For a port, the port-specific configuration takes priority over the global configuration.

When you configure a rule in the IPv6 ACL, follow these restrictions and guidelines:

- In a basic ACL, the **source** *source-address source-prefix* option specifies an IPv6 multicast group address.
- In an advanced ACL, the **source** *source-address source-prefix* option specifies an IPv6 multicast source address. The **destination** *dest-address dest-prefix* option specifies an IPv6 multicast group address.

  To match MLDv1 reports, set the **source** *source-address source-prefix* option to 0::0.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

You can configure different ACLs for all ports in different VLANs. If you configure multiple ACLs for all ports in the same VLAN, the most recent configuration takes effect.

Examples

Configure an IPv6 multicast group policy for VLAN 2 so that hosts in VLAN 2 can join only IPv6 multicast group FF03::101.

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2000
[Sysname-acl-ipv6-basic-2000] rule permit source ff03::101 128
[Sysname-acl-ipv6-basic-2000] quit
[Sysname] mld-snooping
[Sysname-mld-snooping] group-policy 2000 vlan 2
```

Related commands

mld-snooping group-policy

host-aging-time (MLD-snooping view)

Use **host-aging-time** to set the aging timer for dynamic member ports globally.

Use **undo host-aging-time** to restore the default.

Syntax

host-aging-time *seconds*

undo host-aging-time

Default

The aging timer for dynamic member ports is 260 seconds.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

seconds: Specifies an aging timer for dynamic member ports, in the range of 1 to 8097894 seconds.

Usage guidelines

You can set the timer globally for all VLANs in MLD-snooping view or for a VLAN in VLAN view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

To avoid mistakenly deleting IPv6 multicast group members, set the aging timer for dynamic member ports to be greater than the value calculated by using the following formula:

[MLD general query interval] + [maximum response time for MLD general queries]

As a best practice, set the aging timer of dynamic member ports to the value calculated by using the following formula:

[MLD general query interval] × 2 + [maximum response time for MLD general queries]

Examples

Set the global aging timer for dynamic member ports to 300 seconds.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] host-aging-time 300
```

Related commands

mld-snooping host-aging-time

host-tracking (MLD-snooping view)

Use **host-tracking** to enable host tracking globally.

Use **undo host-tracking** to disable host tracking globally.

Syntax

host-tracking

undo host-tracking

Default

Host tracking is disabled.

Views

MLD-snooping view

Predefined user roles

network-admin

Usage guidelines

You can enable host tracking globally for all VLANs in MLD-snooping view or for a VLAN in VLAN view. For a VLAN, the global configuration has the same priority as the VLAN-specific configuration.

Examples

Enable host tracking globally.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] host-tracking
```

Related commands

display mld-snooping host-tracking

mld-snooping host-tracking

last-listener-query-interval (MLD-snooping view)

Use **last-listener-query-interval** to set the MLD last listener query interval globally.

Use **undo last-listener-query-interval** to restore the default.

Syntax

last-listener-query-interval *interval*

undo last-listener-query-interval

Default

The MLD last listener query interval is 1 second.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

interval: Specifies an MLD last listener query interval in the range of 1 to 25 seconds.

Usage guidelines

You can set the interval for a VLAN in VLAN view or globally for all VLANs in MLD-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

Examples

Set the global MLD last listener query interval to 3 seconds.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] last-listener-query-interval 3
```

Related commands

mld-snooping last-listener-query-interval

max-response-time (MLD-snooping view)

Use **max-response-time** to set the maximum response time for MLD general queries globally.

Use **undo max-response-time** to restore the default.

Syntax

max-response-time *seconds*

undo max-response-time

Default

The maximum response time for MLD general queries is 10 seconds.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

seconds: Specifies the maximum response time for MLD general queries, in the range of 1 to 3174 seconds.

Usage guidelines

You can set the time globally for all VLANs in MLD-snooping view or for a VLAN in VLAN view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

To avoid mistakenly deleting IPv6 multicast group members, set the maximum response time for MLD general queries to be less than the MLD general query interval.

Examples

Set the global maximum response time for MLD general queries to 5 seconds.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] max-response-time 5
```

Related commands

mld-snooping max-response-time

mld-snooping query-interval

mld-snooping

Use **mld-snooping** to enable the MLD snooping feature and enter MLD-snooping view.

Use **undo mld-snooping** to disable the MLD snooping feature.

Syntax

mld-snooping

undo mld-snooping

Default

The MLD snooping feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

If you disable the MLD snooping feature, MLD snooping is disabled in all VLANs.

Examples

Enable the MLD snooping feature and enter MLD-snooping view.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping]
```

Related commands

enable (MLD-snooping view)

mld-snooping enable

mld-snooping disable

mld-snooping access-policy

Use **mld-snooping access-policy** to configure an MLD snooping access control policy.

Use **undo mld-snooping access-policy** to delete an MLD snooping access control policy.

Syntax

mld-snooping access-policy *ipv6-acl-number*

undo mld-snooping access-policy { *ipv6-acl-number* | **all** }

Default

No MLD snooping access control policies exist. IPv6 multicast users can join or leave any IPv6 multicast groups.

Views

User profile view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies an IPv6 basic or advanced ACL by its number, in the range of 2000 to 3999. IPv6 multicast users can join only the IPv6 multicast groups that the ACL permits. If the ACL does not exist or does not have valid rules, IPv6 multicast users cannot join or leave any IPv6 multicast groups.

all: Specifies all MLD snooping access control policies.

Usage guidelines

You can repeat this command to configure multiple MLD snooping access control policies. An IPv6 multicast user can join or leave an IPv6 multicast group if its MLD report or done message is permitted by one of the MLD snooping access control policies.

When you configure a rule in the IPv6 ACL, follow these restrictions and guidelines:

- In a basic ACL, the **source** *source-address source-prefix* option specifies an IPv6 multicast group address.
- In an advanced ACL, the **source** *source-address source-prefix* option specifies an IPv6 multicast source address. The **destination** *dest-address dest-prefix* option specifies an IPv6 multicast group address.

  To match the following MLD messages, set the **source** *source-address source-prefix* option to 0::0:

  - MLDv1 report and done messages.
  - MLDv2 IS_EX and MLDv2 TO_EX reports that do not carry IPv6 multicast source addresses.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

Examples

In user profile **abc**, configure an MLD snooping access control policy to allow IPv6 multicast users to join or leave only IPv6 multicast group FF03::101.

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2001
[Sysname-acl6-basic-2001] rule permit source ff03::101 16
[Sysname-acl6-basic-2001] quit
[Sysname] user-profile abc
[Sysname-user-profile-abc] mld-snooping access-policy 2001
```

mld-snooping done source-ip

Use **mld-snooping done source-ip** to configure the source IPv6 address for MLD done messages.

Use **undo mld-snooping done source-ip** to restore the default.

Syntax

mld-snooping done source-ip *ipv6-address*

undo mld-snooping done source-ip

Default

In a VLAN, the source IPv6 address of MLD done messages is the IPv6 link-local address of the current VLAN interface. If the current VLAN interface does not have an IPv6 link-local address, the source IPv6 address is FE80::02FF:FFFF:FE00:0001.

Views

VLAN view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the source IPv6 address for MLD done messages.

Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command.

Examples

In VLAN 2, enable MLD snooping, and specify FE80:0:0:1::1 as the source IPv6 address of MLD done messages.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping done source-ip fe80:0:0:1::1
```

Related commands

enable (MLD-snooping view)

mld-snooping enable

mld-snooping dot1p-priority

Use **mld-snooping dot1p-priority** to set the 802.1p priority for MLD messages in a VLAN.

Use **undo mld-snooping dot1p-priority** to restore the default.

Syntax

mld-snooping dot1p-priority *priority*

undo mld-snooping dot1p-priority

Default

The 802.1p priority is 6 for MLD messages in a VLAN.

Views

VLAN view

Predefined user roles

network-admin

Parameters

priority: Specifies an 802.1p priority for MLD messages, in the range of 0 to 7. The greater the value, the higher the priority.

Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command.

You can set the 802.1p priority for a VLAN in VLAN view or globally for all VLANs in MLD-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

Examples

In VLAN 2, enable MLD snooping, and set the 802.1p priority for MLD messages to 3.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping dot1p-priority 3
```

Related commands

dot1p-priority (MLD-snooping view)

enable (MLD-snooping view)

mld-snooping enable

mld-snooping drop-unknown

Use **mld-snooping drop-unknown** to enable dropping unknown IPv6 multicast data packets for a VLAN.

Use **undo mld-snooping drop-unknown** to disable dropping unknown IPv6 multicast data packets for a VLAN.

Syntax

mld-snooping drop-unknown

undo mld-snooping drop-unknown

Default

Dropping unknown IPv6 multicast data packets is disabled. Unknown IPv6 multicast data packets are flooded.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command.

Examples

In VLAN 2, enable MLD snooping, and enable dropping unknown IPv6 multicast data packets.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping drop-unknown
```

Related commands

enable (MLD-snooping view)

mld-snooping enable

mld-snooping { disable | enable }

Use **mld-snooping enable** to enable MLD snooping for a VLAN.

Use **mld-snooping disable** to disable MLD snooping for a VLAN.

Use **undo mld-snooping** to restore the MLD snooping status in a VLAN to the global MLD snooping status.

Syntax

mld-snooping { **disable** | **enable** }

undo mld-snooping

Default

The MLD snooping status in a VLAN is consistent with the global MLD snooping status.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

You must enable the MLD snooping feature by using the **mld-snooping** command before you enable MLD snooping for a VLAN.

You can enable MLD snooping for a VLAN by using this command in VLAN view or for multiple VLANs by using the **enable** command. The configuration in VLAN view has the same priority as the configuration in MLD-snooping view, and the most recent configuration takes effect.

Examples

Enable the MLD snooping feature, and then enable MLD snooping for VLAN 2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
```

Disable MLD snooping for VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping disable
```

Related commands

enable (MLD-snooping view)

mld-snooping

mld-snooping fast-leave

Use **mld-snooping fast-leave** to enable fast-leave processing on a port.

Use **undo mld-snooping fast-leave** to disable fast-leave processing on a port.

Syntax

mld-snooping fast-leave [**vlan** *vlan-list*]

undo mld-snooping fast-leave [**vlan** *vlan-list*]

Default

Fast-leave processing is disabled on a port.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

The fast-leave processing feature enables the device to immediately remove a port from the forwarding entry for an IPv6 multicast group when the port receives a done message.

You can enable fast-leave processing for a port in interface view or globally for all ports in MLD-snooping view. For a port, the port-specific configuration takes priority over the global configuration.

Examples

Enable fast-leave processing for VLAN 2 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping fast-leave vlan 2
```

Related commands

fast-leave (MLD-snooping view)

mld-snooping general-query source-ip

Use **mld-snooping general-query source-ip** to configure the source IPv6 address for MLD general queries.

Use **undo mld-snooping general-query source-ip** to restore the default.

Syntax

mld-snooping general-query source-ip *ipv6-address*

undo mld-snooping general-query source-ip

Default

In a VLAN, the source IPv6 address for MLD general queries is the IPv6 link-local address of the current VLAN interface. If the current VLAN interface does not have an IPv6 link-local address, the source IPv6 address is FE80::02FF:FFFF:FE00:0001.

Views

VLAN view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the source IPv6 address for MLD general queries.

Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command.

Examples

In VLAN 2, enable MLD snooping, and specify FE80:0:0:1::1 as the source IPv6 address for MLD general queries.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping general-query source-ip fe80:0:0:1::1
```

Related commands

enable (MLD-snooping view)

mld-snooping enable

mld-snooping group-limit

Use **mld-snooping group-limit** to set the maximum number of IPv6 multicast groups that a port can join.

Use **undo mld-snooping group-limit** to remove the limit on the maximum number of IPv6 multicast groups that a port can join.

Syntax

mld-snooping group-limit *limit* [**vlan** *vlan-list*]

undo mld-snooping group-limit [**vlan** *vlan-list*]

Default

No limit is placed on the maximum number of IPv6 multicast groups that a port can join.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

limit: Specifies the maximum number of multicast groups that a port can join, in the range of 0 to 4294967295.

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect for all VLANs.

Usage guidelines

This command takes effect only on the IPv6 multicast groups that a port joins dynamically.

Examples

On GigabitEthernet 1/0/1, set the maximum number to 10 for IPv6 multicast groups that the port can join in VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping group-limit 10 vlan 2
```

mld-snooping group-policy

Use **mld-snooping group-policy** to configure an IPv6 multicast group policy on a port to control the IPv6 multicast groups that hosts attached to the port can join.

Use **undo mld-snooping group-policy** to delete IPv6 multicast group policies on a port.

Syntax

mld-snooping group-policy *ipv6-acl-number* [**vlan** *vlan-list*]

undo mld-snooping group-policy [**vlan** *vlan-list*]

Default

No IPv6 multicast group policies exist. Hosts attached to the port can join any IPv6 multicast groups.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies an IPv6 basic or advanced ACL number in the range of 2000 to 3999. Hosts can join only the IPv6 multicast groups that the ACL permits. If the ACL does not exist or does not have valid rules, hosts cannot join IPv6 multicast groups.

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

An IPv6 multicast group policy filters MLD reports to control the IPv6 multicast groups that hosts can join.

This command does not take effect on static member ports, because static member ports do not send MLD reports.

You can configure an IPv6 multicast group policy for a port in interface view or globally for all ports in MLD-snooping view. For a port, the port-specific configuration takes priority over the global configuration.

When you configure a rule in the IPv6 ACL, follow these restrictions and guidelines:

- In a basic ACL, the **source** *source-address source-prefix* option specifies an IPv6 multicast group address.
- In an advanced ACL, the **source** *source-address source-prefix* option specifies an IPv6 multicast source address. The **destination** *dest-address dest-prefix* option specifies an IPv6 multicast group address.

  To match MLDv1 reports and MLD IS_EX and MLDv2 TO_EX reports that do not carry IPv6 multicast source addresses, set the **source** *source-address source-prefix* option to 0::0.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

You can configure different ACLs for different VLANs on a port. If you configure multiple ACLs for the same VLANs on a port, the most recent configuration takes effect.

Examples

On GigabitEthernet 1/0/1, configure an IPv6 multicast group policy for VLAN 2 so that hosts attached to the port in VLAN 2 can join only the group FF03::101.

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2000
[Sysname-acl-ipv6-basic-2000] rule permit source ff03::101 128
[Sysname-acl-ipv6-basic-2000] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping group-policy 2000 vlan 2
```

Related commands

group-policy (MLD-snooping view)

mld-snooping host-aging-time

Use **mld-snooping host-aging-time** to set the aging timer for dynamic member ports in a VLAN.

Use **undo mld-snooping host-aging-time** to restore the default.

Syntax

mld-snooping host-aging-time *seconds*

undo mld-snooping host-aging-time

Default

The aging timer for dynamic member ports is 260 seconds.

Views

VLAN view

Predefined user roles

network-admin

Parameters

seconds: Specifies an aging timer for dynamic member ports, in the range of 1 to 8097894 seconds.

Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command.

You can set the timer for a VLAN in VLAN view or globally for all VLANs in MLD-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

To avoid mistakenly deleting IPv6 multicast group members, set the aging timer for dynamic member ports to be greater than the value calculated by using the following formula:

[MLD general query interval] + [maximum response time for MLD general queries]

As a best practice, set the aging timer of dynamic member ports to the value calculated by using the following formula:

[MLD general query interval] × 2 + [maximum response time for MLD general queries]

Examples

In VLAN 2, enable MLD snooping, and set the aging timer for dynamic member ports in the VLAN to 300 seconds.

```
<Sysname> system-view
```

```
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping host-aging-time 300
```

Related commands

enable (MLD-snooping view)

host-aging-time (MLD-snooping view)

mld-snooping enable

mld-snooping host-join

Use **mld-snooping host-join** to configure a port as a simulated member host for an IPv6 multicast group or an IPv6 multicast source and group.

Use **undo mld-snooping host-join** to remove the configuration of a simulated member host for an IPv6 multicast group.

Syntax

mld-snooping host-join *ipv6-group-address* [**source-ip** *ipv6-source-address*] **vlan** *vlan-id*

undo mld-snooping host-join { *ipv6-group-address* [**source-ip** *ipv6-source-address*] **vlan** *vlan-id* | **all** }

Default

A port is not a simulated member host of any IPv6 multicast groups or any IPv6 multicast sources and groups.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

source-ip *ipv6-source-address*: Specifies an IPv6 multicast source by its IPv6 address. If you specify an IPv6 multicast source, this command configures the port as a simulated member host for an IPv6 multicast source and group. If you do not specify an IPv6 multicast source, this command configures the port as a simulated member host for an IPv6 multicast group. This option takes effect on MLDv2 snooping devices.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

all: Specifies all IPv6 multicast groups and all IPv6 multicast sources and groups.

Usage guidelines

The version of MLD running on a simulated member host is the same as the version of MLD snooping running on the port. The port ages out in the same way as a dynamic member port.

Examples

Configure GigabitEthernet 1/0/1 as a simulated member host for the IPv6 multicast group (*, FF3E::101) in VLAN 2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping host-join ff3e::101 vlan 2
```

mld-snooping host-tracking

Use **mld-snooping host-tracking** to enable host tracking for a VLAN.

Use **undo mld-snooping host-tracking** to disable host tracking for a VLAN.

Syntax

mld-snooping host-tracking

undo mld-snooping host-tracking

Default

Host tracking is disabled.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command for the VLAN.

You can enable host tracking for a VLAN in VLAN view or globally for all VLANs in MLD-snooping view. For a VLAN, the VLAN-specific configuration has the same priority as the global configuration.

Examples

In VLAN 2, enable MLD snooping, and then enable host tracking.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping host-tracking
```

Related commands

display mld-snooping host-tracking

host-tracking (MLD-snooping view)

mld-snooping enable

mld-snooping last-listener-query-interval

Use **mld-snooping last-listener-query-interval** to set the MLD last listener query interval for a VLAN.

Use **undo mld-snooping last-listener-query-interval** to restore the default.

Syntax

mld-snooping last-listener-query-interval *interval*

undo mld-snooping last-listener-query-interval

Default

The MLD last listener query interval is 1 second.

Views

VLAN view

Predefined user roles

network-admin

Parameters

interval: Specifies an MLD last listener query interval in the range of 1 to 25 seconds.

Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command.

You can set the interval for a VLAN in VLAN view or globally for all VLANs in MLD-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

Examples

In VLAN 2, enable MLD snooping, and set the MLD last listener query interval to 3 seconds.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping last-listener-query-interval 3
```

Related commands

enable (MLD-snooping view)

last-listener-query-interval (MLD-snooping view)

mld-snooping enable

mld-snooping max-response-time

Use **mld-snooping max-response-time** to set the maximum response time for MLD general queries in a VLAN.

Use **undo mld-snooping max-response-time** to restore the default.

Syntax

mld-snooping max-response-time *seconds*

undo mld-snooping max-response-time

Default

The maximum response time for MLD general queries is 10 seconds.

Views

VLAN view

Predefined user roles

network-admin

Parameters

seconds: Specifies the maximum response time for MLD general queries, in the range of 1 to 3174 seconds.

Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command.

You can set the time for a VLAN in VLAN view or globally for all VLANs in MLD-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

To avoid mistakenly deleting IPv6 multicast group members, set the maximum response time for MLD general queries to be less than the MLD general query interval.

Examples

In VLAN 2, enable MLD snooping, and set the maximum response time for MLD general queries to 5 seconds.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping max-response-time 5
```

Related commands

enable (MLD-snooping view)

max-response-time (MLD-snooping view)

mld-snooping enable

mld-snooping query-interval

mld-snooping overflow-replace

Use **mld-snooping overflow-replace** to enable the IPv6 multicast group replacement feature on a port.

Use **undo mld-snooping overflow-replace** to disable the multicast group replacement feature on a port.

Syntax

mld-snooping overflow-replace [**vlan** *vlan-list*]

undo mld-snooping overflow-replace [**vlan** *vlan-list*]

Default

The IPv6 multicast group replacement feature is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

This command takes effect only on the IPv6 multicast groups that a port joins dynamically.

You can enable the IPv6 multicast group replacement feature for a port in interface view or globally for all ports in MLD-snooping view. For a port, the port-specific configuration takes priority over the global configuration.

Examples

On GigabitEthernet 1/0/1, enable the IPv6 multicast group replacement feature for VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping overflow-replace vlan 2
```

Related commands

overflow-replace (MLD-snooping view)

mld-snooping proxy enable

Use **mld-snooping proxy enable** to enable MLD snooping proxying for a VLAN.

Use **undo mld-snooping proxy enable** to disable MLD snooping proxying for a VLAN.

Syntax

mld-snooping proxy enable

undo mld-snooping proxy enable

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command.

This command does not take effect on a VLAN that is a sub-VLAN of an IPv6 multicast VLAN.

Examples

In VLAN 2, enable MLD snooping, and enable MLD snooping proxying.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
```

```
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping proxy enable
```

Related commands

enable (MLD-snooping view)

mld-snooping enable

subvlan (IPv6 multicast-VLAN view)

mld-snooping querier

Use **mld-snooping querier** to enable the MLD snooping querier.

Use **undo mld-snooping querier** to disable the MLD snooping querier.

Syntax

mld-snooping querier

undo mld-snooping querier

Default

The MLD snooping querier is disabled.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command.

For a sub-VLAN of an IPv6 multicast VLAN, this command takes effect only after you remove the VLAN from the IPv6 multicast VLAN.

Examples

In VLAN 2, enable MLD snooping, and enable the MLD snooping querier.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping querier
```

Related commands

enable (MLD-snooping view)

mld-snooping enable

subvlan (IPv6 multicast-VLAN view)

mld-snooping querier-election

Use **mld-snooping querier-election** to enable MLD snooping querier election for a VLAN.

Use **undo mld-snooping querier-election** to disable MLD snooping querier election for a VLAN.

Syntax

mld-snooping querier-election

undo mld-snooping querier-election

Default

MLD snooping querier election is disabled.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command.

For MLD snooping querier election to take effect, you must enable the MLD snooping querier.

Examples

In VLAN 2, enable MLD snooping, and enable MLD snooping querier election.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping querier
[Sysname-vlan2] mld-snooping querier-election
```

Related commands

mld-snooping querier

mld-snooping query-interval

Use **mld-snooping query-interval** to set the MLD general query interval for a VLAN.

Use **undo mld-snooping query-interval** to restore the default.

Syntax

mld-snooping query-interval *interval*

undo mld-snooping query-interval

Default

The MLD general query interval is 125 seconds.

Views

VLAN view

Predefined user roles

network-admin

Parameters

interval: Specifies an MLD general query interval, in the range of 2 to 31744 seconds.

Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command for the VLAN.

To avoid mistakenly deleting IPv6 multicast group members, set the MLD general query interval to be greater than the maximum response time for MLD general queries.

Examples

In VLAN 2, enable MLD snooping, and set the MLD general query interval to 20 seconds.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping query-interval 20
```

Related commands

enable (MLD-snooping view)

max-response-time

mld-snooping enable

mld-snooping max-response-time

mld-snooping querier

mld-snooping report source-ip

Use **mld-snooping report source-ip** to configure the source IPv6 address for MLD reports.

Use **undo mld-snooping report source-ip** to restore the default.

Syntax

mld-snooping report source-ip *ipv6-address*

undo mld-snooping report source-ip

Default

In a VLAN, the source IPv6 address for MLD reports is the IPv6 link-local address of the current VLAN interface. If the current VLAN interface does not have an IPv6 link-local address, the source IPv6 address is FE80::02FF:FFFF:FE00:0001.

Views

VLAN view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the source IPv6 address for MLD reports.

Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command.

Examples

In VLAN 2, enable MLD snooping, and specify FE80:0:0:1::1 as the source IPv6 address for MLD reports.

```
<Sysname> system-view
```

```
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping report source-ip fe80:0:0:1::1
```

Related commands

enable (MLD-snooping view)

mld-snooping enable

mld-snooping router-aging-time

Use **mld-snooping router-aging-time** to set the aging timer for dynamic router ports in a VLAN.

Use **undo mld-snooping router-aging-time** to restore the default.

Syntax

mld-snooping router-aging-time *seconds*

undo mld-snooping router-aging-time

Default

The aging timer for dynamic router ports is 260 seconds.

Views

VLAN view

Predefined user roles

network-admin

Parameters

seconds: Specifies an aging timer for dynamic router ports, in the range of 1 to 8097894 seconds.

Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command.

You can set the timer for a VLAN in VLAN view or globally for all VLANs in MLD-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

Examples

In VLAN 2, enable MLD snooping, and set the aging timer for dynamic router ports in the VLAN to 100 seconds.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping router-aging-time 100
```

Related commands

enable (MLD-snooping view)

mld-snooping enable

router-aging-time (MLD-snooping view)

mld-snooping router-port-deny

Use **mld-snooping router-port-deny** to disable a port from becoming a dynamic router port.

Use **undo mld-snooping router-port-deny** to allow a port to become a dynamic router port.

Syntax

mld-snooping router-port-deny [**vlan** *vlan-list*]

undo mld-snooping router-port-deny [**vlan** *vlan-list*]

Default

A port is allowed to become a dynamic router port.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you specify VLANs, this command takes effect only when the port belongs to the specified VLANs. If you do not specify a VLAN, this command takes effect on all VLANs.

Examples

Disable GigabitEthernet 1/0/1 from becoming a dynamic router port in VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping router-port-deny vlan 2
```

mld-snooping source-deny

Use **mld-snooping source-deny** to enable IPv6 multicast source port filtering on a port to discard all IPv6 multicast data packets.

Use **undo mld-snooping source-deny** to disable IPv6 multicast source port filtering on a port.

Syntax

mld-snooping source-deny

undo mld-snooping source-deny

Default

IPv6 multicast source port filtering is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

You can enable this feature for a port in interface view or for the specified ports in MLD-snooping view. For a port, the configuration in interface view has the same priority as the configuration in MLD-snooping view, and the most recent configuration takes effect.

Examples

Enable source port filtering for IPv6 multicast data on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping source-deny
```

Related commands

source-deny (MLD-snooping view)

mld-snooping special-query source-ip

Use **mld-snooping special-query source-ip** to configure the source IPv6 address for MLD multicast-address-specific queries.

Use **undo mld-snooping special-query source-ip** to restore the default.

Syntax

mld-snooping special-query source-ip *ipv6-address*

undo mld-snooping special-query source-ip

Default

In a VLAN, the source IPv6 address of MLD multicast-address-specific queries is one of the following:

- The source address of MLD general queries if the MLD snooping querier of the VLAN has received MLD general queries.
- The IPv6 link-local address of the current VLAN interface if the MLD snooping querier does not receive an MLD general query.
- FE80::02FF:FFFF:FE00:0001 if the MLD snooping querier does not receive an MLD general query and the current VLAN interface does not have an IPv6 link-local address.

Views

VLAN view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the source IPv6 address for MLD multicast-address-specific queries.

Usage guidelines

You must enable MLD snooping for a VLAN before you execute this command.

Examples

In VLAN 2, enable MLD snooping, and specify FE80:0:0:1::1 as the source IPv6 address of MLD multicast-address-specific queries.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
```

```
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping special-query source-ip fe80:0:0:1::1
```

Related commands

enable (MLD-snooping view)

mld-snooping enable

mld-snooping static-group

Use **mld-snooping static-group** to configure a port as a static member port of an IPv6 multicast group or an IPv6 multicast source and group.

Use **undo mld-snooping static-group** to delete the configuration of static member ports.

Syntax

mld-snooping static-group *ipv6-group-address* [**source-ip** *ipv6-source-address*] **vlan** *vlan-id*

undo mld-snooping static-group { *ipv6-group-address* [**source-ip** *ipv6-source-address*] **vlan** *vlan-id* | **all** }

Default

A port is not a static member port of IPv6 multicast groups.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

source-ip *ipv6-source-address*: Specifies an IPv6 multicast source by its IPv6 address. If you specify an IPv6 multicast source, this command configures the port as a static member port of an IPv6 multicast source and group. If you do not specify an IPv6 multicast source, this command configures the port as a static member port of an IPv6 multicast group. This option takes effect on MLDv2 snooping devices.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

all: Specifies all IPv6 multicast groups and all IPv6 multicast sources and groups.

Examples

Configure GigabitEthernet 1/0/1 as a static member port for the IPv6 multicast group (*, FF3E::101) in VLAN 2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] quit
```

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping static-group ff3e::101 vlan 2
```

mld-snooping static-router-port

Use **mld-snooping static-router-port** to configure a port as a static router port.

Use **undo mld-snooping static-router-port** to remove the configuration of static router ports.

Syntax

mld-snooping static-router-port vlan *vlan-id*

undo mld-snooping static-router-port { **all** | **vlan** *vlan-id* }

Default

A port is not a static router port.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

all: Specifies all VLANs.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

Examples

Configure GigabitEthernet 1/0/1 as a static router port in VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping static-router-port vlan 2
```

mld-snooping version

Use **mld-snooping version** to specify an MLD snooping version for a VLAN.

Use **undo mld-snooping version** to restore the default.

Syntax

mld-snooping version *version-number*

undo mld-snooping version

Default

The MLD snooping version in a VLAN is 1.

Views

VLAN view

Predefined user roles

network-admin

Parameters

version-number: Specifies an MLD snooping version, 1 or 2.

Usage guidelines

You must enable MLD snooping for a VLAN before you configure this command.

You can specify the version for a VLAN in VLAN view or for the specified VLANs in MLD-snooping view. The VLAN-specific configuration has the same priority as the configuration in MLD-snooping view, and the most recent configuration takes effect.

Examples

In VLAN 2, enable MLD snooping, and specify MLD snooping version 2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping version 2
```

Related commands

enable (MLD-snooping view)

mld-snooping enable

version (MLD-snooping view)

overflow-replace (MLD-snooping view)

Use **overflow-replace** to enable the IPv6 multicast group replacement feature globally.

Use **undo overflow-replace** to disable the IPv6 multicast group replacement feature globally.

Syntax

overflow-replace [**vlan** *vlan-list*]

undo overflow-replace [**vlan** *vlan-list*]

Default

The IPv6 multicast group replacement feature is disabled.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

This command takes effect only on the IPv6 multicast groups that a port joins dynamically.

You can enable IPv6 multicast group replacement globally for all ports in MLD-snooping view or for a port in interface view. For a port, the port-specific configuration takes priority over the global configuration.

Examples

Globally enable the IPv6 multicast group replacement feature for VLAN 2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] overflow-replace vlan 2
```

Related commands

mld-snooping overflow-replace

report-aggregation (MLD-snooping view)

Use **report-aggregation** to enable MLD report suppression.

Use **undo report-aggregation** to disable MLD report suppression.

Syntax

report-aggregation

undo report-aggregation

Default

MLD report suppression is enabled.

Views

MLD-snooping view

Predefined user roles

network-admin

Examples

Disable MLD report suppression.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] undo report-aggregation
```

reset ipv6 l2-multicast fast-forwarding cache

Use **reset ipv6 l2-multicast fast-forwarding cache** to clear Layer 2 IPv6 multicast fast forwarding entries.

Syntax

reset ipv6 l2-multicast fast-forwarding cache [**vlan** *vlan-id*] { { *ipv6-source-address* | *ipv6-group-address* } * | **all** } [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

Parameters

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

ipv6-source-address: Specifies an IPv6 multicast source address.

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears Layer 2 IPv6 multicast fast forwarding entries for the master device.

all: Specifies all Layer 2 IPv6 multicast fast forwarding entries.

Examples

Clear all Layer 2 IPv6 multicast fast forwarding entries.

```
<Sysname> reset ipv6 l2-multicast fast-forwarding cache all
```

Clear the Layer 2 IPv6 multicast fast forwarding entry for the IPv6 group (*, FF1E::2).

```
<Sysname> reset ipv6 l2-multicast fast-forwarding cache FF1E::2
```

Related commands

display ipv6 l2-multicast fast-forwarding cache

reset mld-snooping group

Use **reset mld-snooping group** to clear information about dynamic MLD snooping group entries.

Syntax

reset mld-snooping group { *ipv6-group-address* [*ipv6-source-address*] | **all** } [**vlan** *vlan-id*]

Views

User view

Predefined user roles

network-admin

Parameters

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

ipv6-source-address: Specifies an IPv6 multicast source address. If you do not specify an IPv6 multicast source, this command clears information about dynamic MLD snooping group entries for all IPv6 multicast sources.

all: Specifies all IPv6 multicast groups.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command clears information about dynamic MLD snooping group entries for all VLANs.

Examples

Clear information about all dynamic MLD snooping group entries.

```
<Sysname> reset mld-snooping group all
```

Related commands

display mld-snooping group

reset mld-snooping router-port

Use **reset mld-snooping router-port** to clear dynamic router port information.

Syntax

reset mld-snooping router-port { **all** | **vlan** *vlan-id* }

Views

User view

Predefined user roles

network-admin

Parameters

all: Specifies all dynamic router ports.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command clears dynamic router port information for all VLANs.

Examples

Clear information about all dynamic router ports.

```
<Sysname> reset mld-snooping router-port all
```

Related commands

display mld-snooping router-port

reset mld-snooping statistics

Use **reset mld-snooping statistics** to clear statistics for MLD messages and IPv6 PIM hello messages learned through MLD snooping.

Syntax

reset mld-snooping statistics

Views

User view

Predefined user roles

network-admin

Examples

Clear statistics for all MLD messages and IPv6 PIM hello messages learned through MLD snooping.

```
<Sysname> reset mld-snooping statistics
```

Related commands

display mld-snooping statistics

router-aging-time (MLD-snooping view)

Use **router-aging-time** to set the aging timer for dynamic router ports globally.

Use **undo router-aging-time** to restore the default.

Syntax

router-aging-time *seconds*

undo router-aging-time

Default

The aging timer for dynamic router ports is 260 seconds.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

seconds: Specifies an aging timer for dynamic router ports, in the range of 1 to 8097894 seconds.

Usage guidelines

You can set the timer globally for all VLANs in MLD-snooping view or for a VLAN in VLAN view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

Examples

Set the global aging timer for dynamic router ports to 100 seconds.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] router-aging-time 100
```

Related commands

mld-snooping router-aging-time

source-deny (MLD-snooping view)

Use **source-deny** to enable IPv6 multicast source port filtering on ports to discard all IPv6 multicast data packets.

Use **undo source-deny** to disable IPv6 multicast source port filtering on ports.

Syntax

source-deny port *interface-list*

undo source-deny port *interface-list*

Default

IPv6 multicast source port filtering is disabled.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

port *interface-list*: Specifies a space-separated list of port items. Each item specifies a port by its port type and number or a range of ports in the form of *start-interface-type interface-number* **to** *end-interface-type interface-number*.

Usage guidelines

You can enable this feature for the specified ports in MLD-snooping view or for a port in interface view. For a port, the configuration in MLD-snooping view has the same priority as the configuration in interface view, and the most recent configuration takes effect.

Examples

Enable source port filtering for IPv6 multicast data on ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] source-deny port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

Related commands

mld-snooping source-deny

version (MLD-snooping view)

Use **version** to specify an MLD snooping version for VLANs.

Use **undo version** to restore the default.

Syntax

version *version-number* **vlan** *vlan-list*

undo version vlan *vlan-list*

Default

The MLD snooping version in a VLAN is 1.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

version-number: Specifies an MLD snooping version, 1 or 2.

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094.

Usage guidelines

You must enable MLD snooping for the specified VLANs before you execute this command.

You can specify the version for the specified VLANs in MLD-snooping view or for a VLAN in VLAN view. The VLAN-specific configuration has the same priority as the configuration in MLD-snooping view, and the most recent configuration takes effect.

Examples

Enable MLD snooping for VLAN 2 through VLAN 10, and specify MLD snooping version 2 for these VLANs.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] enable vlan 2 to 10
[Sysname-mld-snooping] version 2 vlan 2 to 10
```

Related commands

`enable` (MLD-snooping view)

`mld-snooping enable`

`mld-snooping version`

Contents

IPv6 PIM snooping commands

display ipv6 pim-snooping neighbor

Use **display ipv6 pim-snooping neighbor** to display IPv6 PIM snooping neighbor information.

Syntax

display ipv6 pim-snooping neighbor [**vlan** *vlan-id*] [**slot** *slot-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays IPv6 PIM snooping neighbor information for all VLANs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 PIM snooping neighbor information for the master device.

verbose: Displays detailed information about IPv6 PIM snooping neighbors. If you do not specify this keyword, the command displays brief information about IPv6 PIM snooping neighbors.

Examples

Display detailed information about IPv6 PIM snooping neighbors for VLAN 2.

```
<Sysname> display ipv6 pim-snooping neighbor vlan 2 verbose
Total 2 neighbors.

VLAN 2: Total 2 neighbors.
  FE80::6401:101
    Slots (0 in total):
    Ports (1 in total):
      GE1/0/1                             (02:02:23)    LAN Prune Delay(T)
  FE80::C801:101
    Slots (0 in total):
    Ports (1 in total):
      GE1/0/2                             (02:02:25)
```

Table 1 Command output

Field	Description
Total 2 neighbors	Total number of IPv6 PIM snooping neighbors.
VLAN 2: Total 2 neighbors	Total number of IPv6 PIM snooping neighbors in VLAN 2.
FE80::6401:101	IPv6 address of the IPv6 PIM snooping neighbor.
Slots (0 in total)	Member IDs and total number of the member devices that have the

Field	Description
	neighbor, except for the specified member device or the master device when no member device is specified.
Ports (1 in total)	Ports where IPv6 PIM snooping neighbors reside, and the total number of the ports.
(02:02:23)	Remaining aging time for an IPv6 PIM snooping neighbor on the port. This field is always displayed for a global port (such as Layer 2 aggregate interfaces). For a non-global port, this field is displayed when one of the following conditions exists: • The port is on the specified member device. • The port is on the master device and no member device is specified.
LAN Prune Delay	IPv6 PIM hello message sent by the IPv6 PIM snooping neighbor has the LAN_Prune_Delay option.
(T)	The join report suppression feature has been disabled for the IPv6 PIM snooping neighbor.

display ipv6 pim-snooping router-port

Use **display ipv6 pim-snooping router-port** to display IPv6 PIM snooping router port information.

Syntax

display ipv6 pim-snooping router-port [**vlan** *vlan-id*] [**slot** *slot-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays IPv6 PIM snooping router port information for all VLANs.

verbose: Displays detailed information about IPv6 PIM snooping router ports. If you do not specify this keyword, the command displays brief information about IPv6 PIM snooping router ports.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 PIM snooping router port information for the master device.

Examples

Display brief information about IPv6 PIM snooping router ports for VLAN 2.

```
<Sysname> display ipv6 pim-snooping router-port vlan 2
VLAN 2:
  Router ports (2 in total):
    GE1/0/1                                 (00:01:30)
    GE1/0/2                                 (00:01:32)
```

Display detailed information about IPv6 PIM snooping router ports for VLAN 2.

```
<Sysname> display ipv6 pim-snooping router-port vlan 2 verbose
VLAN 2:
  Router slots (0 in total):
  Router ports (2 in total):
    GE1/0/1                             (00:01:30)
    GE1/0/2                             (00:01:32)
```

Table 2 Command output

Field	Description
VLAN 2	VLAN ID.
Router slots (0 in total)	Member IDs and total number of the member devices that have router ports, except for the specified member device or the master device when no member device is specified.
Router ports (2 in total)	Router ports and total number of router ports.
(00:01:30)	Remaining aging time for the router port. For a global port, this field is always displayed. For a non-global port, this field is displayed when one of the following conditions exists: • The port is on the specified member device. • The port is on the master device and no member device is specified.

display ipv6 pim-snooping routing-table

Use **display ipv6 pim-snooping routing-table** to display IPv6 PIM snooping routing entries.

Syntax

display ipv6 pim-snooping routing-table [**vlan** *vlan-id*] [**slot** *slot-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays IPv6 PIM snooping routing entries for all VLANs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 PIM snooping routing entries for the master device.

verbose: Displays detailed information about IPv6 PIM snooping routing entries. If you do not specify this keyword, the command displays brief information about IPv6 PIM snooping routing entries.

Examples

Display detailed information about IPv6 PIM snooping routing entries for VLAN 2.

```
<Sysname> display ipv6 pim-snooping routing-table vlan 2 verbose
```

```
Total 1 entries.
FSM Flag: NI-no info, J-join, PP-prune pending

VLAN 2: Total 1 entries.
  (2000::1, FF1E::1)
    FSM information: dummy
    Upstream neighbor: FE80::101
      Upstream Slots (0 in total):
      Upstream Ports (1 in total):
        GE1/0/1
      Downstream Slots (0 in total):
      Downstream Ports (2 in total):
        GE1/0/2
          Expires: 00:03:01, FSM: J
          Downstream Neighbors (2 in total):
            1001::1
              Expires: 00:59:19, FSM: J
            1001::2
              Expires: 00:59:20, FSM: J
        GE1/0/3
          Expires: 00:02:21, FSM: PP
```

Table 3 Command output

Field	Description
Total 1 entries	Total number of (S, G) and (*, G) entries.
FSM Flag: NI-no info, J-join, PP-prune pending	State machine flag of the downstream port: • **NI**—Initial state. • **J**—Join. • **PP**—Prune pending.
VLAN 2: Total 1 entries	Total number of (S, G) entries in VLAN 2.
(2000::1, FF1E::1)	(S, G) entry.
FSM information	Finite state machine information for the entry: • **delete**—The entry attributes have been deleted. • **dummy**—The entry is a new temporary entry. • **no info**—The entry does not exist. • **normal**—The entry is a correct entry.
Upstream neighbor	Upstream neighbor of the (S, G) or (*, G) entry.
Upstream Slots (0 in total)	Member IDs and total number of the member devices that have the upstream neighbor, except for the specified member device or the master device when no member device is specified.
Upstream Ports (1 in total)	Upstream ports, and the total number of the ports. This field is displayed when one of the following conditions exists: • The port is on the specified member device. • The port is on the master device and no member device is specified.
Downstream Slots (0 in total)	Member IDs and total number of the member devices that have downstream ports, except for the specified member device or the master device when no member device is specified.

Field	Description
Downstream Ports (2 in total)	Downstream ports of the upstream neighbor, and the total number of the ports.
Downstream Neighbors (2 in total)	Downstream neighbors of the downstream port, and the total number of the neighbors.
Expires: 00:03:01, FSM: J	Remaining aging time for the downstream port or downstream neighbor, and the finite sate machine information. For a global port, this field is always displayed. For a non-global port, this field is displayed when one of the following conditions exists: • The port is on the specified member device. • The port is on the master device and no member device is specified.

display ipv6 pim-snooping statistics

Use **display ipv6 pim-snooping statistics** to display statistics for the IPv6 PIM messages learned through IPv6 PIM snooping.

Syntax

display ipv6 pim-snooping statistics

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display statistics for the IPv6 PIM messages learned through IPv6 PIM snooping.

```
<Sysname> display ipv6 pim-snooping statistics
Received IPv6 PIM hello:  100
Received IPv6 PIM join/prune:  100
Received IPv6 PIM error:  0
Received IPv6 PIM messages in total:  200
```

Table 4 Command output

Field	Description
Received IPv6 PIM hello	Number of received IPv6 PIM hello messages.
Received IPv6 PIM join/prune	Number of received IPv6 PIM join/prune messages.
Received IPv6 PIM error	Number of received IPv6 PIM messages with errors.
Received IPv6 PIM messages in total	Total number of received IPv6 PIM messages.

Related commands

reset ipv6 pim-snooping statistics

ipv6 pim-snooping enable

Use **ipv6 pim-snooping enable** to enable IPv6 PIM snooping for a VLAN.

Use **undo ipv6 pim-snooping enable** to disable IPv6 PIM snooping for a VLAN.

Syntax

ipv6 pim-snooping enable

undo ipv6 pim-snooping enable

Default

IPv6 PIM snooping is disabled for a VLAN.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

IPv6 PIM snooping does not take effect on sub-VLANs of IPv6 multicast VLANs.

You must enable the MLD snooping feature and enable MLD snooping for a VLAN before you execute this command.

Examples

Enable the MLD snooping feature, and then enable MLD snooping and IPv6 PIM snooping for VLAN 2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] ipv6 pim-snooping enable
```

Related commands

mld-snooping

mld-snooping enable

ipv6 pim-snooping graceful-restart join-aging-time

Use **ipv6 pim-snooping graceful-restart join-aging-time** to set the aging time for global downstream ports and global router ports on the new master device after a master/subordinate switchover.

Use **undo ipv6 pim-snooping graceful-restart join-aging-time** to restore the default.

Syntax

ipv6 pim-snooping graceful-restart join-aging-time *seconds*

undo ipv6 pim-snooping graceful-restart join-aging-time

Default

The aging time is 210 seconds for global downstream ports and global router ports on the new master device after a master/subordinate switchover.

Views

VLAN view

Predefined user roles

network-admin

Parameters

seconds: Specifies an aging time in the range of 210 to 18000 seconds.

Usage guidelines

You must enable IPv6 PIM snooping for a VLAN before you execute this command.

Global ports include Layer 2 aggregate interfaces. A global downstream port or a global router port is a global port that acts as a downstream port or router port, respectively.

Examples

In VLAN 2, set the aging time to 300 seconds for global downstream ports and global router ports on the new master device after a master/subordinate switchover.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] ipv6 pim-snooping enable
[Sysname-vlan2] ipv6 pim-snooping graceful-restart join-aging-time 300
```

Related commands

ipv6 pim-snooping enable

ipv6 pim-snooping graceful-restart neighbor-aging-time

Use **ipv6 pim-snooping graceful-restart neighbor-aging-time** to set the aging time for global neighbor ports on the new master device after a master/subordinate switchover.

Use **undo ipv6 pim-snooping graceful-restart neighbor-aging-time** to restore the default.

Syntax

ipv6 pim-snooping graceful-restart neighbor-aging-time *seconds*

undo ipv6 pim-snooping graceful-restart neighbor-aging-time

Default

The aging time is 105 seconds for global neighbor ports on the new master device after a master/subordinate switchover.

Views

VLAN view

Predefined user roles

network-admin

Parameters

seconds: Specifies an aging time in the range of 105 to 18000 seconds.

Usage guidelines

You must enable IPv6 PIM snooping for a VLAN before you execute this command.

Global ports include Layer 2 aggregate interfaces. A global neighbor port is a global port that acts as a neighbor port.

Examples

In VLAN 2, set the aging time to 300 seconds for global neighbor ports on the new master device after a master/subordinate switchover.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] ipv6 pim-snooping enable
[Sysname-vlan2] ipv6 pim-snooping graceful-restart neighbor-aging-time 300
```

Related commands

ipv6 pim-snooping enable

reset ipv6 pim-snooping statistics

Use **reset ipv6 pim-snooping statistics** to clear statistics for the IPv6 PIM messages learned through IPv6 PIM snooping.

Syntax

reset ipv6 pim-snooping statistics

Views

User view

Predefined user roles

network-admin

Examples

Clear statistics for the IPv6 PIM messages learned through IPv6 PIM snooping.

```
<Sysname> reset ipv6 pim-snooping statistics
```

Related commands

display ipv6 pim-snooping statistics

Contents

IPv6 multicast VLAN commands

display ipv6 multicast-vlan

Use **display ipv6 multicast-vlan** to display information about IPv6 multicast VLANs.

Syntax

display ipv6 multicast-vlan [*vlan-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan-id: Specifies an IPv6 multicast VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify an IPv6 multicast VLAN, this command displays information about all IPv6 multicast VLANs.

Examples

Display information about all IPv6 multicast VLANs.

```
<Sysname> display ipv6 multicast-vlan
Total 2 IPv6 multicast VLANs.

IPv6 multicast VLAN 100:
  Sub-VLAN list(3 in total):
    2-3, 6
  Port list(3 in total):
    GE1/0/1
    GE1/0/2
    GE1/0/3

IPv6 multicast VLAN 200:
  Sub-VLAN list(0 in total):
  Port list(0 in total):
```

Table 1 Command output

Field	Description
Total 2 IPv6 multicast VLANs	Total number of IPv6 multicast VLANs.
Sub-VLAN list(3 in total)	Sub-VLAN list of the IPv6 multicast VLAN, and the total number of the sub-VLANs.
Port list(3 in total)	Port list of the IPv6 multicast VLAN, and the total number of the ports.

display ipv6 multicast-vlan forwarding-table

Use **display ipv6 multicast-vlan forwarding-table** to display IPv6 multicast VLAN forwarding entries.

Syntax

display ipv6 multicast-vlan forwarding-table [*ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **slot** *slot-number* | **subvlan** *vlan-id* | **vlan** *vlan-id*] *

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6-source-address: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, this command displays IPv6 multicast VLAN forwarding entries for all IPv6 multicast sources.

prefix-length: Specifies a prefix length of the IPv6 multicast source address. The value range is 0 to 128 and the default value is 128.

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16, where "x" and "y" represent any hexadecimal numbers in the range of 0 to F. If you do not specify an IPv6 multicast group, this command displays IPv6 multicast VLAN forwarding entries for all IPv6 multicast groups.

prefix-length: Specifies a prefix length of the IPv6 multicast group address. The value range is 8 to 128 and the default value is 128.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 multicast VLAN forwarding entries for the master device.

subvlan *vlan-id*: Specifies a sub-VLAN by its VLAN ID. If you do not specify a sub-VLAN, this command displays IPv6 multicast VLAN forwarding entries for all sub-VLANs.

vlan *vlan-id*: Specifies an IPv6 multicast VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify an IPv6 multicast VLAN, this command displays IPv6 multicast VLAN forwarding entries for all VLANs.

Examples

Display all IPv6 multicast VLAN forwarding entries.

```
<Sysname> display ipv6 multicast-vlan forwarding-table
IPv6 multicast VLAN 100 Forwarding Table
Total 1 entries, 1 matched

00001. (1::1, FF0E::1)
     Flags: 0x10000
     IPv6 multicast VLAN: 100
     List of sub-VLANs (3 in total):
       1: VLAN 10
       2: VLAN 20
       3: VLAN 30
```

Table 2 Command output

Field	Description
IPv6 multicast VLAN 100 Forwarding Table	The multicast forwarding table for IPv6 multicast VLAN 100.
Total 1 entries, 1 matched	Total number of (S, G) entries, and the number of matching entries.
00001	Sequence number of the (S, G) entry.
(1::1, FF0E::1)	(S, G) entry, where a double colon (::) in the S position means all IPv6 multicast sources.
Flags	Entry flag. This field displays one flag or the sum of multiple flags. In this example, the value 0x10000 means that the entry has only one flag 0x10000. The following flags are available for an entry: • **0x1**—The entry is in inactive state. • **0x4**—The entry fails to update. • **0x8**—The sub-VLAN information fails to update for the entry. • **0x200**—The entry is in GR state. • **0x10000**—The entry is an IPv6 multicast VLAN forwarding entry.
List of sub-VLANs (3 in total)	Sub-VLAN list of the IPv6 multicast VLAN, and the total number of the sub-VLANs.

display ipv6 multicast-vlan group

Use **display ipv6 multicast-vlan group** to display information about IPv6 multicast groups in IPv6 multicast VLANs.

Syntax

display ipv6 multicast-vlan group [*ipv6-source-address* | *ipv6-group-address* | **slot** *slot-number* | **verbose** | **vlan** *vlan-id*] *

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6-source-address: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, this command displays information about IPv6 multicast groups for all IPv6 multicast sources in IPv6 multicast VLANs.

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F. If you do not specify an IPv6 multicast group, this command displays information about all IPv6 multicast groups in IPv6 multicast VLANs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about IPv6 multicast groups in IPv6 multicast VLANs for the master device.

verbose: Displays detailed information. If you do not specify the keyword, this command displays brief information.

vlan *vlan-id*: Specifies an IPv6 multicast VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify an IPv6 multicast VLAN, this command displays information about IPv6 multicast groups for all IPv6 multicast VLANs.

Examples

Display detailed information about all IPv6 multicast groups in IPv6 multicast VLANs.

```
<Sysname> display ipv6 multicast-vlan group verbose
Total 6 entries.

IPv6 multicast VLAN 10: Total 3 entries.
  (2::2, FF0E::2)
    Flags: 0x70000020
    Sub-VLANs (1 in total):
      VLAN 40
  (22::22, FF0E::4)
    Flags: 0x70000030
    Sub-VLANs (1 in total):
      VLAN 40
  (::, FF0E::10)
    Flags: 0x10000030
    Sub-VLANs (1 in total):
      VLAN 40

IPv6 multicast VLAN 20: Total 3 entries.
  (2::2, FF0E::2)
    Flags: 0x70000010
    Sub-VLANs (0 in total):
  (22::22, FF0E::4)
    Flags: 0x70000010
    Sub-VLANs (0 in total):
  (::, FF0E::10)
    Flags: 0x50000010
    Sub-VLANs (0 in total):
```

Table 3 Command output

Field	Description
Total 6 entries	Total number of (S, G) entries.
IPv6 multicast VLAN 10: Total 3 entries	Total number of (S, G) entries in IPv6 multicast VLAN 10.
(::, FF0E::10)	(S, G) entry, where a double colon (::) in the S position means all IPv6 multicast sources.
Flags	Entry flag. This field displays one flag or the sum of multiple flags. For example, the value 0x70000020 means that the entry has flags 0x20, 0x10000000, 0x20000000, and 0x40000000. The following flags are available for an entry: • **0x10**—The entry is created by the IPv6 multicast VLAN. • **0x20**—The entry is created by the sub-VLAN of the IPv6

Field	Description

	multicast VLAN.
	• **0x40**—The entry is to be deleted.
	• **0x10000000**—This value represents one of the following situations:
	  ○ The entry is newly created.
	  ○ The device receives an MLD query within an MLD general query interval.
	• **0x20000000**—The device does not receive MLDv1 or MLDv2 reports that match the entry within an MLD general query interval.
	• **0x40000000**—The device does not receive MLDv2 IS_EX (NULL) reports that match the entry within an MLD general query interval.

Sub-VLANs (1 in total)	Sub-VLAN list of the IPv6 multicast VLAN, and the total number of the sub-VLANs.

Related commands

reset ipv6 multicast-vlan group

ipv6 multicast-vlan

Use **ipv6 multicast-vlan** to configure an IPv6 multicast VLAN and enter its view, or enter the view of an existing IPv6 multicast VLAN.

Use **undo ipv6 multicast-vlan** to remove the configuration of IPv6 multicast VLANs.

Syntax

ipv6 multicast-vlan *vlan-id*

undo ipv6 multicast-vlan { **all** | *vlan-id* }

Default

No IPv6 multicast VLANs exist.

Views

System view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies an existing VLAN ID in the range of 1 to 4094.

all: Specifies all IPv6 multicast VLANs.

Usage guidelines

The total number of IPv6 multicast VLANs on the device cannot exceed 5.

You must enable MLD snooping for the VLAN to be configured as an IPv6 multicast VLAN.

Examples

Enable MLD snooping for VLAN 100. Configure VLAN 100 as an IPv6 multicast VLAN and enter its view.

```
<Sysname> system-view
[Sysname] mld-snooping
```

```
[Sysname-mld-snooping] quit
[Sysname] vlan 100
[Sysname-vlan100] mld-snooping enable
[Sysname-vlan100] quit
[Sysname] ipv6 multicast-vlan 100
[Sysname-ipv6-mvlan-100]
```

Related commands

mld-snooping enable

ipv6 multicast-vlan entry-limit

Use **ipv6 multicast-vlan entry-limit** to set the maximum number of IPv6 multicast VLAN forwarding entries.

Use **undo ipv6 multicast-vlan entry-limit** to restore the default.

Syntax

ipv6 multicast-vlan entry-limit *limit*

undo ipv6 multicast-vlan entry-limit

Default

The following matrix shows the default values for the maximum number of IPv6 multicast VLAN forwarding entries:

Hardware	Maximum number of multicast VLAN forwarding entries
S5110V2-SI switch series S5000V3-EI switch series S5000V5-EI switch series S5000E-X switch series S5000X-EI switch series S5110V2 switch series WS5810-WiNet switch series	60
S5120V2-LI switch series S5130S-LI switch series S5120V3-SI switch series MS4320V2 switch series MS4320 switch series	120
WAS6000 switch series	• WAS6124 and WAS6148: 500 • Other switches: 240
S3100V3-SI switch series	• Switches with product code LS-3100V3-18TP-SI-H1, LS-3100V3-28TP-SI-H1, LS-3100V3-52TP-SI-H1, or LS-3100V3-20TP-PWR-SI-H1: 60 • Other switches: 120
MS4200 switch series	• Switches with product code LS-MS4200-28TP-H1, LS-MS4200-18TP-H1, or LS-MS4200-20TP-PWR-H1: 60 • Other switches: 120

WS5820-WiNet switch series	• Switches with product code WS5820-28P-POE-WiNet: 60 • Other switches: 120
MS4300V2 switch series	• MS4300V2-28P, MS4300V2-52P: 60 • MS4300V2-10P: 120
MS4320V3 switch series	• MS4320V3-28P, MS4320V3-52P: 60 • Other switches: 120
S5120V3-LI switch series	• S5120V2-20P-LI, S5120V2-28P-LI, S5120V2-52P-LI, S5120V2-28P-PWR-LI, S5120V2-52P-PWR-LI: 60 • Other switches: 120

Views

System view

Predefined user roles

network-admin

Parameters

limit: Specifies the maximum number of IPv6 multicast VLAN forwarding entries. The following matrix shows the value range for this argument:

Hardware	Value range
S5110V2-SI switch series S5000V3-EI switch series S5000V5-EI switch series S5000E-X switch series S5000X-EI switch series WAS6000 switch series S5110V2 switch series WS5810-WiNet switch series	0 to 60
S5120V2-LI switch series S5130S-LI switch series S5120V3-SI switch series MS4320V2 switch series MS4320 switch series	0 to 120
S3100V3-SI switch series	• Switches with product code LS-3100V3-18TP-SI-H1, LS-3100V3-28TP-SI-H1, LS-3100V3-52TP-SI-H1, or LS-3100V3-20TP-PWR-SI-H1: 0 to 60 • Other switches: 0 to 120
MS4200 switch series	• Switches with product code LS-MS4200-28TP-H1, LS-MS4200-18TP-H1, or LS-MS4200-20TP-PWR-H1: 0 to 60 • Other switches: 0 to 120
WS5820-WiNet switch series	• Switches with product code WS5820-28P-POE-WiNet: 0 to 60 • Other switches: 0 to 120

MS4300V2 switch series	• MS4300V2-28P, MS4300V2-52P: 0 to 60 • MS4300V2-10P: 0 to 120
MS4320V3 switch series	• MS4320V3-28P, MS4320V3-52P: 0 to 60 • Other switches: 0 to 120
S5120V3-LI switch series	• S5120V2-20P-LI, S5120V2-28P-LI, S5120V2-52P-LI, S5120V2-28P-PWR-LI, S5120V2-52P-PWR-LI: 0 to 60 • Other switches: 0 to 120

Usage guidelines

If the configured value is smaller than the current number of IPv6 multicast VLAN forwarding entries, the device cannot create new entries until some entries age out or are manually removed. To allow new entries to be created immediately, use the **reset ipv6 multicast-vlan group** command to remove IPv6 multicast VLAN forwarding entries.

Examples

Set the maximum number of IPv6 multicast VLAN forwarding entries to 120.

```
<Sysname> system-view
[Sysname] ipv6 multicast-vlan entry-limit 120
```

Related commands

entry-limit (MLD-snooping view)

ipv6 port multicast-vlan

Use **ipv6 port multicast-vlan** to assign a user port to an IPv6 multicast VLAN.

Use **undo ipv6 port multicast-vlan** to restore the default.

Syntax

ipv6 port multicast-vlan *vlan-id*

undo ipv6 port multicast-vlan

Default

A port does not belong to an IPv6 multicast VLAN.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies an IPv6 multicast VLAN by its VLAN ID in the range of 1 to 4094.

Usage guidelines

You can assign a port to only one IPv6 multicast VLAN.

For the port to be assigned to an IPv6 multicast VLAN, you must enable MLD snooping for the VLAN to which the port belongs.

Examples

Assign GigabitEthernet 1/0/1 to IPv6 multicast VLAN 100.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 port multicast-vlan 100
```

port (IPv6 multicast VLAN view)

Use **port** to assign user ports to an IPv6 multicast VLAN.

Use **undo port** to delete user ports from an IPv6 multicast VLAN.

Syntax

port *interface-list*

undo port { **all** | *interface-list* }

Default

An IPv6 multicast VLAN does not have user ports.

Views

IPv6 multicast VLAN view

Predefined user roles

network-admin

Parameters

interface-list: Specifies a port in the form of *interface-type interface-number*, or a port range in the form of *interface-type interface-number* to *interface-type interface-number*.

all: Specifies all user ports in the current IPv6 multicast VLAN.

Usage guidelines

You can assign only Layer 2 Ethernet interfaces or Layer 2 aggregate interfaces as user ports to an IPv6 multicast VLAN. Additionally, you can assign a port to only one IPv6 multicast VLAN.

For ports to be assigned to an IPv6 multicast VLAN, you must enable MLD snooping for the VLANs to which the ports belong.

Examples

Assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5 as user ports to IPv6 multicast VLAN 100.

```
<Sysname> system-view
[Sysname] ipv6 multicast-vlan 100
[Sysname-ipv6-mvlan-100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/5
```

reset ipv6 multicast-vlan group

Use **reset ipv6 multicast-vlan group** to clear IPv6 multicast group entries in IPv6 multicast VLANs.

Syntax

reset ipv6 multicast-vlan group [*ipv6-group-address* [*prefix-length*] | *ipv6-source-address* [*prefix-length*] | **vlan** *vlan-id*] *

Views

User view

Predefined user roles

network-admin

Parameters

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F. If you do not specify an IPv6 multicast group, this command clears all IPv6 multicast group entries in IPv6 multicast VLANs.

prefix-length: Specifies a prefix length of the IPv6 multicast group address. The value range is 8 to 128 and the default value is 128.

ipv6-source-address: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, this command clears IPv6 multicast group entries for all IPv6 multicast sources in IPv6 multicast VLANs.

prefix-length: Specifies a prefix length of the IPv6 multicast source address. The value range is 0 to 128 and the default value is 128.

vlan *vlan-id*: Specifies an IPv6 multicast VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify an IPv6 multicast VLAN, this command clears IPv6 multicast group entries for all IPv6 multicast VLANs.

Examples

Clear all IPv6 multicast group entries for all IPv6 multicast VLANs.

```
<Sysname> reset ipv6 multicast-vlan group
```

Related commands

display ipv6 multicast-vlan group

subvlan (IPv6 multicast VLAN view)

Use **subvlan** to assign VLANs as sub-VLANs to an IPv6 multicast VLAN.

Use **undo subvlan** to delete sub-VLANs from an IPv6 multicast VLAN.

Syntax

subvlan *vlan-list*

undo subvlan { **all** | *vlan-list* }

Default

An IPv6 multicast VLAN does not have sub-VLANs.

Views

IPv6 multicast VLAN view

Predefined user roles

network-admin

Parameters

vlan-list: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The value range for the VLAN ID is 1 to 4094. The specified VLANs must exist and cannot be multicast VLANs or sub-VLANs of other IPv6 multicast VLANs.

all: Specifies all sub-VLANs of the current IPv6 multicast VLAN.

Usage guidelines

You must enable MLD snooping for VLANs to be configured as sub-VLANs of an IPv6 multicast VLAN.

Examples

Assign VLAN 10 through VLAN 15 as sub-VLANs to multicast VLAN 100.

```
<Sysname> system-view
[Sysname] ipv6 multicast-vlan 100
[Sysname-ipv6-mvlan-100] subvlan 10 to 15
```

ACL and QoS Command Reference

This command reference is applicable to the following switches and software versions:

H3C S5120V2-LI switch series (Release 6308P01 and later)
H3C S3100V3-SI switch series (Release 6309P01 and later)
H3C S5110V2 switch series (Release 6310 and later)
H3C S5110V2-SI switch series (Release 6310 and later)
H3C S5000V3-EI switch series (Release 6310 and later)
H3C S5000V5-EI switch series (Release 6319P01 and later)
H3C S5000E-X switch series (Release 6310 and later)
H3C S5130S-LI switch series (Release 6310 and later)
H3C MS4320V2 switch series (Release 6308P01 and later)
H3C MS4320 switch series (Release 6308P01 and later)
H3C MS4300V2 switch series (Release 6308P01 and later)
H3C MS4200 switch series (Release 6310 and later)
H3C WS5810-WiNet switch series (Release 6308P01 and later)
H3C WS5820-WiNet switch series (Release 6308P01 and later)
H3C WAS6000 switch series (Release 6308P01 and later)
H3C S5000X-EI switch series (Release 6329 and later)
H3C MS4320V3 switch series (Release 6329 and later)
H3C S5120V3-SI switch series (Release 6329 and later)
H3C S5120V3-LI switch series (Release 6329 and later)

New H3C Technologies Co., Ltd.
http://www.h3c.com

Software version: Release 63xx
Document version: 6W105-20230524

Preface

This command reference describes the ACL and QoS configuration commands.

This preface includes the following topics about the documentation:

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Documentation feedback

You can e-mail your comments about product documentation to info@h3c.com.

We appreciate your comments.

Contents

ACL commands

acl

Use **acl** to create an ACL and enter its view, or enter the view of an existing ACL.

Use **undo acl** to delete the specified or all ACLs.

Syntax

Command set 1:

acl [**ipv6**] { **name** *acl-name* | **number** *acl-number* [**name** *acl-name*] [**match-order** { **auto** | **config** }] }

undo acl [**ipv6**] { **all** | **name** *acl-name* | **number** *acl-number* }

Command set 2:

acl [**ipv6**] { **advanced** | **basic** } { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }]

acl mac { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }]

undo acl [**ipv6**] { **all** | { **advanced** | **basic** } { *acl-number* | **name** *acl-name* } }

undo acl mac { **all** | *acl-number* | **name** *acl-name* }

Default

No ACLs exist.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6: Specifies the IPv6 ACL type. To specify the IPv4 ACL type, do not use this keyword.

basic: Specifies the basic ACL type.

advanced: Specifies the advanced ACL type.

mac: Specifies the Layer 2 ACL type.

number *acl-number*: Assigns a number to the ACL.

acl-number: Assigns a number to the ACL. The following are available value ranges:

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name *acl-name*: Assigns a name to the ACL. The *acl-name* argument is a case-insensitive string of 1 to 63 characters. It must start with an English letter and to avoid confusion, it cannot be **all**.

match-order: Specifies the order in which ACL rules are compared against packets.

- **auto**: Compares ACL rules in depth-first order.

- **config**: Compares ACL rules in ascending order of rule ID. The rule with a smaller ID has a higher priority. If you do not specify a match order, the **config** order applies by default.

all: Specifies all ACLs of the specified type.

Usage guidelines

If you create a numbered ACL, you can enter the view of the ACL by using either of the following commands:

- The **acl** [**ipv6**] **number** *acl-number* command.
- The **acl** { [**ipv6**] { **advanced** | **basic** } | **mac** } *acl-number* command.

If you create a ACL by using the **acl** [**ipv6**] **number** *acl-number* **name** *acl-name* command, you can enter the view of the ACL by using either of the following commands:

- **acl** [**ipv6**] **name** *acl-name* (for only basic ACLs and advanced ACLs).
- **acl** [**ipv6**] **number** *acl-number* [**name** *acl-name*].
- **acl** { [**ipv6**] { **advanced** | **basic** } | **mac**] } **name** *acl-name*.

If you create a named ACL by using the **acl** { [**ipv6**] { **advanced** | **basic** } | **mac** } **name** *acl-name* command, you can enter the view of the ACL by using either of the following commands:

- **acl** [**ipv6**] **name** *acl-name* (for only basic ACLs and advanced ACLs).
- **acl** { [**ipv6**] { **advanced** | **basic** } | **mac** } **name** *acl-name*.

You can change the match order only for ACLs that do not contain any rules.

Matching packets are forwarded through slow forwarding if an ACL rule contains match criteria or has functions enabled in addition to the following match criteria and functions:

- Source and destination IP addresses.
- Source and destination ports.
- Transport layer protocol.
- ICMP or ICMPv6 message type, message code, and message name.
- Logging.
- Time range.

Slow forwarding requires packets to be sent to the control plane for forwarding entry calculation, which affects the device forwarding performance.

Examples

Create IPv4 basic ACL 2000 and enter its view.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000]
```

Create IPv4 basic ACL **flow** and enter its view.

```
<Sysname> system-view
[Sysname] acl basic name flow
[Sysname-acl-ipv4-basic-flow]
```

Create IPv4 advanced ACL 3000 and enter its view.

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000]
```

Create IPv6 basic ACL 2000 and enter its view.

```
<Sysname> system-view
```

```
[Sysname] acl ipv6 basic 2000
[Sysname-acl-ipv6-basic-2000]
```

Create IPv6 basic ACL **flow** and enter its view.

```
<Sysname> system-view
[Sysname] acl ipv6 basic name flow
[Sysname-acl-ipv6-basic-flow]
```

Create IPv6 advanced ACL **abc** and enter its view.

```
<Sysname> system-view
[Sysname] acl ipv6 advanced name abc
[Sysname-acl-ipv6-adv-abc]
```

Create Layer 2 ACL 4000 and enter its view.

```
<Sysname> system-view
[Sysname] acl mac 4000
[Sysname-acl-mac-4000]
```

Create Layer 2 ACL **flow** and enter its view.

```
<Sysname> system-view
[Sysname] acl mac name flow
[Sysname-acl-mac-flow]
```

Related commands

display acl

acl copy

Use **acl copy** to create an ACL by copying an ACL that already exists.

Syntax

acl [**ipv6** | **mac**] **copy** { *source-acl-number* | **name** *source-acl-name* } **to** { *dest-acl-number* | **name** *dest-acl-name* }

Views

System view

Predefined user roles

network-admin

Parameters

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

source-acl-number: Specifies an existing source ACL by its number. The following are available value ranges:

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name *source-acl-name*: Specifies an existing source ACL by its name. The *source-acl-name* argument is a case-insensitive string of 1 to 63 characters.

dest-acl-number: Assigns a unique number to the new ACL. The following are available value ranges:

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name *dest-acl-name*: Assigns a unique name to the new ACL. The *dest-acl-name* argument is a case-insensitive string of 1 to 63 characters. It must start with an English letter and to avoid confusion, it cannot be **all**.

Usage guidelines

The new ACL and the source ACL must be the same type.

When specifying an ACL by its number, follow these rules:

- To specify an IPv6 ACL, you must specify both its ACL number and the **ipv6** keyword.
- To specify a Layer 2 ACL, you can specify its ACL number without the **mac** keyword.

To specify an IPv6 ACL or Layer 2 ACL by a name, you must specify both the ACL name and the **ipv6** or **mac** keyword.

The new ACL has the same properties and content as the source ACL, but uses a different number or name from the source ACL.

Examples

Create IPv4 basic ACL 2002 by copying IPv4 basic ACL 2001.

```
<Sysname> system-view
[Sysname] acl copy 2001 to 2002
```

Create IPv4 basic ACL **paste** by copying IPv4 basic ACL **test**.

```
<Sysname> system-view
[Sysname] acl copy name test to name paste
```

acl logging interval

Use **acl logging interval** to enable logging for packet filtering and set the interval.

Use **undo acl logging interval** to restore the default.

Syntax

acl logging interval *interval*

undo acl logging interval

Default

The interval is 0. The device does not generate log entries for packet filtering.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the interval at which log entries are generated and output. It must be a multiple of 5, in the range of 0 to 1440 minutes. To disable the logging, set the value to 0.

Usage guidelines

The logging feature is available for IPv4 or IPv6 ACL rules that have the **logging** keyword.

You can configure the ACL module to generate log entries for packet filtering and output them to the information center at the output interval. The log entry records the number of matching packets and the matched ACL rules. When the first packet of a flow matches an ACL rule, the output interval starts, and the device immediately outputs a log entry for this packet. When the output interval ends, the device outputs a log entry for subsequent matching packets of the flow. For more information about the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Configure the device to generate and output packet filtering log entries every 10 minutes.

```
<Sysname> system-view
[Sysname] acl logging interval 10
```

Related commands

rule (IPv4 advanced ACL view)

rule (IPv4 basic ACL view)

rule (IPv6 advanced ACL view)

rule (IPv6 basic ACL view)

acl trap interval

Use **acl trap interval** to enable SNMP notifications for packet filtering and set the interval.

Use **undo acl interval** to restore the default.

Syntax

acl trap interval *interval*

undo acl trap interval

Default

The interval is 0. The device does not generate SNMP notifications for packet filtering.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the interval at which SNMP notifications are generated and output. It must be a multiple of 5, in the range of 0 to 1440 minutes. To disable SNMP notifications, set the value to 0.

Usage guidelines

The SNMP notifications feature is available for IPv4 or IPv6 ACL rules that have the **logging** keyword.

You can configure the ACL module to generate SNMP notifications for packet filtering and output them to the SNMP module at the output interval. The notification records the number of matching packets and the matched ACL rules. When the first packet of a flow matches an ACL rule, the output interval starts, and the device immediately outputs a notification for this packet. When the output interval ends, the device outputs a notification for subsequent matching packets of the flow. For more information about SNMP, see *Network Management and Monitoring Configuration Guide*.

Examples

Configure the device to generate and output packet filtering SNMP notifications every 10 minutes.

```
<Sysname> system-view
```

```
[Sysname] acl trap interval 10
```

Related commands

rule (IPv4 advanced ACL view)

rule (IPv4 basic ACL view)

rule (IPv6 advanced ACL view)

rule (IPv6 basic ACL view)

description

Use **description** to configure a description for an ACL.

Use **undo description** to delete an ACL description.

Syntax

description *text*

undo description

Default

An ACL does not have a description.

Views

IPv4 basic/advanced ACL view

IPv6 basic/advanced ACL view

Layer 2 ACL view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 127 characters.

Examples

Configure a description for IPv4 basic ACL 2000.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] description This is an IPv4 basic ACL.
```

Related commands

display acl

display acl

Use **display acl** to display ACL configuration and match statistics.

Syntax

display acl [**ipv6** | **mac**] { *acl-number* | **all** | **name** *acl-name* }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number. The following are available value ranges:

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

all: Specifies all ACLs of the specified type.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters.

Usage guidelines

This command displays ACL rules in **config** or **auto** order, whichever is configured.

To specify the IPv4 ACL type, do not specify the **ipv6** or **mac** keyword.

Examples

Display configuration and match statistics for IPv4 basic ACL 2001.

```
<Sysname> display acl 2001
Basic IPv4 ACL 2001, 1 rule, match-order is auto,
This is an IPv4 basic ACL.
ACL's step is 5, start ID is 0
 rule 5 permit source 1.1.1.1 0
 rule 5 comment This rule is used on GigabitEthernet1/0/1.
```

Display configuration and match statistics for IPv4 advanced ACL **acl1_L4_IN**.

```
<Sysname> display acl name acl1_L4_IN
Advanced IPv4 ACL named acl1_L4_IN, 1 rule,
This is a dynamic advanced IPv4 ACL.
ACL's step is 5, start ID is 0
 rule 0 permit source 1.1.1.1 0
```

Table 1 Command output

Field	Description
Basic IPv4 ACL 2001	Type and number of the ACL. The following field information is about IPv4 basic ACL 2001.
1 rule	The ACL contains one rule.
match-order is auto	The match order for the ACL is **auto**, which sorts ACL rules in depth-first order. This field is not displayed when the match order is **config**.
This is an IPv4 basic ACL.	Description of the ACL.
ACL's step is 5	The rule numbering step is 5.
start ID is 0	The start rule ID is 0.
rule 5 permit source 1.1.1.1 0	Content of rule 5. The rule permits packets sourced from the IP address 1.1.1.1.

rule 5 comment This rule is used on GigabitEthernet1/0/1.	Comment of rule 5.
This is a dynamic advanced IPv4 ACL.	The ACL is added dynamically by an application module. This type of ACL can only be added, modified, or deleted by an application module and cannot be configured through CLI commands. This type of ACL is supported only in Release 6309P01 and later.

display packet-filter

Use **display packet-filter** to display ACL application information for packet filtering.

Syntax

display packet-filter interface [*interface-type interface-number*] [**inbound** | **outbound**] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface [*interface-type interface-number*]: Specifies an interface by its type and number. If you do not specify an interface, this command displays ACL application information for packet filtering on all interfaces. If you specify an Ethernet interface, you do not need to specify the **slot** *slot-number* option.

inbound: Specifies the inbound direction.

outbound: Specifies the outbound direction.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays ACL application information for packet filtering for the master device.

Usage guidelines

If neither the **inbound** keyword nor the **outbound** keyword is specified, this command displays ACL application information for packet filtering in both directions.

Examples

Display ACL application information for inbound packet filtering on interface GigabitEthernet 1/0/1.

```
<Sysname> display packet-filter interface gigabitethernet 1/0/1 inbound
Interface: GigabitEthernet1/0/1
 Inbound policy:
  IPv4 ACL 2001r
  IPv6 ACL 2002 (Failed)
  MAC ACL 4003
```

Table 1 Command output

Field	Description
Interface	Interface to which the ACL applies.

Inbound policy	ACL used for filtering incoming traffic.
Outbound policy	ACL used for filtering outgoing traffic.
IPv4 ACL 2001	IPv4 basic ACL 2001 has been successfully applied.
IPv6 ACL 2002 (Failed)	The device has failed to apply IPv6 basic ACL 2002.
Hardware-count	ACL rule match counting in hardware has been successfully enabled.
Hardware-count (Failed)	The device has failed to enable counting ACL rule matches in hardware.
IPv4 default action	Packet filter default action for packets that do not match any IPv4 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.
IPv6 default action	Packet filter default action for packets that do not match any IPv6 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.
MAC default action	Packet filter default action for packets that do not match any Layer 2 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.

display packet-filter statistics

Use **display packet-filter statistics** to display packet filtering statistics.

Syntax

display packet-filter statistics interface *interface-type interface-number* { **inbound** | **outbound** } [[**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }] [**brief**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

inbound: Specifies the inbound direction.

outbound: Specifies the outbound direction.

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number. The following are available value ranges:

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters.

brief: Displays brief statistics.

Usage guidelines

If *acl-number*, **name** *acl-name*, **ipv6**, or **mac** is not specified, this command displays packet filtering statistics for all ACLs.

To specify the IPv4 ACL type, do not specify the **ipv6** or **mac** keyword.

Examples

Display packet filtering statistics for all ACLs on incoming packets of GigabitEthernet 1/0/1.

```
<Sysname> display packet-filter statistics interface gigabitethernet 1/0/1 inbound
Interface: GigabitEthernet1/0/1
 Inbound policy:
  IPv4 ACL 2001, Hardware-count
   From 2011-06-04 10:25:21 to 2011-06-04 10:35:57
   rule 0 permit source 2.2.2.2 0 (2 packets)
   rule 5 permit source 1.1.1.1 0 (Failed)
   Totally 2 packets permitted, 0 packets denied
   Totally 100% permitted, 0% denied

  IPv6 ACL 2000

  MAC ACL 4000
   rule 0 permit
```

Table 2 Command output

Field	Description
Interface	Interface to which the ACL applies.
Inbound policy	ACL used for filtering incoming traffic.
Outbound policy	ACL used for filtering outgoing traffic.
IPv4 ACL 2001	IPv4 basic ACL 2001 has been successfully applied.
IPv4 ACL 2002 (Failed)	The device has failed to apply IPv4 basic ACL 2002.

Hardware-count	ACL rule match counting in hardware has been successfully enabled.
Hardware-count (Failed)	The device has failed to enable counting ACL rule matches in hardware.
From 2011-06-04 10:25:21 to 2011-06-04 10:35:57	Start time and end time of the statistics. The start time is the time when the packet filter was deployed to the member device.
2 packets	Two packets matched the rule. This field is not displayed when no packets matched the rule.
No resource	Resources are not enough for counting matches for the rule. In packet filtering statistics, this field is displayed for a rule when resources are not sufficient for rule match counting.
rule 5 permit source 1.1.1.1 0 (Failed)	The device has failed to apply rule 5.
Totally 2 packets permitted, 0 packets denied	Number of packets permitted and denied by the ACL.
Totally 100% permitted, 0% denied	Ratios of permitted and denied packets to all packets.
IPv4 default action	Packet filter default action for packets that do not match any IPv4 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.
IPv6 default action	Packet filter default action for packets that do not match any IPv6 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.
MAC default action	Packet filter default action for packets that do not match any Layer 2 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.

Related commands

`reset packet-filter statistics`

display packet-filter statistics sum

Use **`display packet-filter statistics sum`** to display accumulated packet filtering statistics for an ACL.

Syntax

display packet-filter statistics sum { **inbound** | **outbound** } [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* } [**brief**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

inbound: Specifies the inbound direction.

outbound: Specifies the outbound direction.

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number.

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters.

brief: Displays brief statistics.

Usage guidelines

To specify the IPv4 ACL type, do not specify the **ipv6** or **mac** keyword.

Examples

Display accumulated packet filtering statistics for IPv4 basic ACL 2001 on incoming packets.

```
<Sysname> display packet-filter statistics sum inbound 2001
Sum:
 Inbound policy:
  IPv4 ACL 2001
   rule 0 permit source 2.2.2.2 0 (2 packets)
   rule 5 permit source 1.1.1.1 0
   Totally 2 packets permitted, 0 packets denied
   Totally 100% permitted, 0% denied
```

Display brief accumulated packet filtering statistics for IPv4 basic ACL 2000 on incoming packets.

```
<Sysname> display packet-filter statistics sum inbound 2000 brief
Sum:
 Inbound policy:
  IPv4 ACL 2000
   Totally 2 packets permitted, 0 packets denied
   Totally 100% permitted, 0% denied
```

Table 3 Command output

Field	Description
Sum	Accumulated packet filtering statistics.
Inbound policy	Accumulated packet filtering statistics in the inbound direction.
Outbound policy	Accumulated packet filtering statistics in the outbound direction.
IPv4 ACL 2001	Accumulated packet filtering statistics of IPv4 basic ACL 2001.
2 packets	Two packets matched the rule. This field is not displayed when no packets matched the rule.
Totally 2 packets permitted, 0 packets denied	Number of packets permitted and denied by the ACL.
Totally 100% permitted, 0% denied	Ratios of permitted and denied packets to all packets.

Related commands

reset packet-filter statistics

display packet-filter verbose

Use **display packet-filter verbose** to display ACL application details for packet filtering.

Syntax

display packet-filter verbose interface *interface-type interface-number* { **inbound** | **outbound** } [[**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. The **slot** *slot-number* option is not available for an Ethernet interface.

inbound: Specifies the inbound direction.

outbound: Specifies the outbound direction.

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number.

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays ACL application details for packet filtering for the master device.

Usage guidelines

If *acl-number*, **name** *acl-name*, **ipv6**, or **mac** is not specified, this command displays application details of all ACLs for packet filtering.

To specify the IPv4 ACL type, do not specify the **ipv6** or **mac** keyword.

Examples

Display application details of all ACLs for inbound packet filtering on GigabitEthernet 1/0/1.

```
<Sysname> display packet-filter verbose interface gigabitethernet 1/0/1 inbound
Interface: GigabitEthernet1/0/1
 Inbound policy:
  IPv4 ACL 2001
   rule 0 permit
   rule 5 permit source 1.1.1.1 0 (Failed)

  IPv6 ACL 2000
   rule 0 permit

  MAC ACL 4000

  IPv4 default action: Deny

  IPv6 default action: Deny, Hardware-count (Failed)

  MAC default action: Deny
```

Table 4 Command output

Field	Description
Interface	Interface to which the ACL applies.
Inbound policy	ACL used for filtering incoming traffic.
Outbound policy	ACL used for filtering outgoing traffic.
IPv4 ACL 2001	IPv4 basic ACL 2001 has been successfully applied.
IPv4 ACL 2002 (Failed)	The device has failed to apply IPv4 basic ACL 2002.
Hardware-count	ACL rule match counting in hardware has been successfully enabled.
Hardware-count (Failed)	The device has failed to enable counting ACL rule matches in hardware.
rule 5 permit source 1.1.1.1 0 (Failed)	The device has failed to apply rule 5.
IPv4 default action	Packet filter default action for packets that do not match any IPv4 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been

	successfully applied for packet filtering.
IPv6 default action	Packet filter default action for packets that do not match any IPv6 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.
MAC default action	Packet filter default action for packets that do not match any Layer 2 ACLs: • **Deny**—The default action **deny** has been successfully applied for packet filtering. • **Deny (Failed)**—The device has failed to apply the default action **deny** for packet filtering. The action **permit** still functions. • **Permit**—The default action **permit** has been successfully applied for packet filtering.

display qos-acl resource

Use **display qos-acl resource** to display QoS and ACL resource usage.

Syntax

display qos-acl resource [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays QoS and ACL resource usage for all member devices.

Usage guidelines

This command does not display any usage data if the specified device does not support counting QoS and ACL resources.

The following features cannot work correctly when QoS and ACL resources are insufficient:

- Packet filtering.
- Device login.
- 802.1X.
- MAC authentication.

For these features to work correctly, reserve enough QoS and ACL resources.

Examples

Display QoS and ACL resource usage.

```
<Sysname> display qos-acl resource
Interfaces: GE1/0/1 to GE1/0/24, XGE1/0/51 to XGE1/0/52 (slot 1)
```

```
-------------------------------------------------------------------------
 Type             Total      Reserved   Configured Remaining  Usage
-------------------------------------------------------------------------
 TTI ACL          256        0          0          256        0%
 PCL ACL          512        16         0          496        3%
 PCL Counter      656        14         0          642        2%
 IPCL Meter       768        0          0          768        0%
 EPCL Meter       128        0          0          128        0%

Interfaces: GE1/0/25 to GE1/0/48, XGE1/0/49 to XGE1/0/50 (slot 1)
-------------------------------------------------------------------------
 Type             Total      Reserved   Configured Remaining  Usage
-------------------------------------------------------------------------
 TTI ACL          256        0          0          256        0%
 PCL ACL          512        16         0          496        3%
 PCL Counter      656        14         0          642        2%
 IPCL Meter       768        0          0          768        0%
 EPCL Meter       128        0          0          128        0%
```

Table 5 Command output

Field	Description
Interfaces	Interface range for the resources.
Type	Resource type: • **TTI ACL**—ACL resources used for interfaces. These resources are used only for QinQ and VLAN mapping in the current software version. • **PCL ACL**—ACL resources used for policies, including resources used by protocol packets and used by the application modules that reference ACLs. • **PCL Counter**—Accounting resources used for policies. • **IPCL Meter**—Traffic policing resources used in inbound QoS policies. • **EPCL Meter**—Traffic policing resources used in outbound QoS policies.
Total	Total number of resources.
Reserved	Number of reserved resources.
Configured	Number of resources that has been applied.
Remaining	Number of resources that you can apply.
Usage	Configured and reserved resources as a percentage of total resources. If the percentage is not an integer, this field displays the integer part. For example, if the actual usage is 50.8%, this field displays 50%.

packet-filter

Use **packet-filter** to apply an ACL to an interface to filter packets.

Use **undo packet-filter** to remove an ACL from an interface.

Syntax

packet-filter [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** } [**hardware-count**]

undo packet-filter [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** }

Default

No ACL is applied to an interface to filter packets.

Views

Layer 2 Ethernet interface view

VLAN interface view

Predefined user roles

network-admin

Parameters

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number.

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters.

inbound: Filters incoming packets.

outbound: Filters outgoing packets.

hardware-count: Enables counting ACL rule matches performed in hardware. If you do not specify this keyword, rule matches for the ACL are not counted in hardware.

Usage guidelines

If you use the *acl-number* argument to specify an ACL, follow these guidelines:

- To specify an IPv4 ACL, use the *acl-number* argument directly.
- To specify an IPv6 ACL, specify the **ipv6** keyword, and then the *acl-number* argument.
- To specify a Layer 2 ACL, the **mac** keyword is not a must. You can either specify the **mac** keyword and then the *acl-number* argument or specify only the *acl-number* argument.

If you use the **name** *acl-name* option to specify an ACL, follow these guidelines:

- To specify an IPv4 ACL, use the **name** *acl-name* option.
- To specify an IPv6 or Layer 2 ACL, specify the related keyword and then the **name** *acl-name* option.

The **hardware-count** keyword in this command enables match counting in hardware for all rules in an ACL, and the **counting** keyword in the **rule** command enables match counting specific to rules.

To disable ACL rule match counting in hardware when resources are insufficient, you must execute the **undo packet-filter** command and then reconfigure the **packet-filter** command without specifying the **hardware-count** keyword.

To disable ACL rule match counting in hardware when resources are sufficient, you can directly reconfigure the **packet-filter** command without specifying the **hardware-count** keyword.

To the same direction of an interface, you can apply a maximum of three ACLs: one IPv4 ACL, one IPv6 ACL, and one Layer 2 ACL.

The inbound packet filtering configured on a VLAN interface filters all packets, including packets forwarded at Layer 3 by the VLAN interface and packets forwarded at Layer 2 by the physical ports associated with the VLAN interface.

The outbound packet filtering configured on a VLAN interface filters only packets forwarded at Layer 3.

Examples

Apply IPv4 basic ACL 2001 to filter incoming traffic on GigabitEthernet 1/0/1, and enable counting ACL rule matches performed in hardware.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] packet-filter 2001 inbound hardware-count
```

Related commands

display packet-filter

display packet-filter statistics

display packet-filter verbose

packet-filter default deny

Use **packet-filter default deny** to set the packet filtering default action to **deny**. The packet filter denies packets that do not match any ACL rule.

Use **undo packet-filter default deny** to restore the default.

Syntax

packet-filter default deny

undo packet-filter default deny

Default

The packet filtering default action is **permit**. The packet filter permits packets that do not match any ACL rule.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The packet filter applies the default action to all ACL applications for packet filtering. The default action appears in the **display** command output for packet filtering.

Examples

Set the packet filter default action to **deny**.

```
<Sysname> system-view
[Sysname] packet-filter default deny
```

Related commands

display packet-filter

display packet-filter statistics

display packet-filter verbose

reset packet-filter statistics

Use **reset packet-filter statistics** to clear the packet filtering statistics.

Syntax

reset packet-filter statistics interface [*interface-type interface-number*] { **inbound** | **outbound** } [[**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }]

Views

User view

Predefined user roles

network-admin

Parameters

interface [*interface-type interface-number*]: Specifies an interface by its type and number. If you do not specify an interface, this command clears packet filtering statistics for all interfaces.

inbound: Specifies the inbound direction.

outbound: Specifies the outbound direction.

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number.

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters.

Usage guidelines

If *acl-number*, **name** *acl-name*, **ipv6**, or **mac** is not specified, this command clears the packet filtering statistics for all ACLs.

To specify the IPv4 ACL type, do not specify the **ipv6** or **mac** keyword.

Examples

Clear IPv4 basic ACL 2001 statistics for inbound packet filtering on GigabitEthernet 1/0/1.

```
<Sysname> reset packet-filter statistics interface gigabitethernet 1/0/1 inbound 2001
```

Related commands

display packet-filter statistics

display packet-filter statistics sum

rule (IPv4 advanced ACL view)

Use **rule** to create or edit an IPv4 advanced ACL rule.

Use **undo rule** to delete an entire IPv4 advanced ACL rule or some attributes in the rule.

Syntax

rule [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { *dest-address dest-wildcard* | **any** } | **destination-port** *operator port* | { **dscp** *dscp* | { **precedence** *precedence* | **tos** *tos* } * } | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | **logging** | **source** { *source-address source-wildcard* | **any** } | **source-port** *operator port* | **time-range** *time-range-name*] *

undo rule *rule-id* [{ { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **established** } | **counting** | **destination** | **destination-port** | { **dscp** | { **precedence** | **tos** } * | **fragment** | **icmp-type** | **logging** | **source** | **source-port** | **time-range**] *

undo rule { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { *dest-address dest-wildcard* | **any** } | **destination-port** *operator port* | { **dscp** *dscp* | { **precedence** *precedence* | **tos** *tos* } * | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | **logging** | **source** { *source-address source-wildcard* | **any** } | **source-port** *operator port* | **time-range** *time-range-name*] *

Default

No IPv4 advanced ACL rules exist.

Views

IPv4 advanced ACL view

Predefined user roles

network-admin

Parameters

rule-id: Specifies a rule ID in the range of 0 to 65534. If you do not specify a rule ID when creating an ACL rule, the system automatically assigns it a rule ID. This rule ID is the nearest higher multiple of the numbering step to the current highest rule ID, starting from the start rule ID. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the rule is numbered 30.

deny: Denies matching packets.

permit: Allows matching packets to pass.

protocol: Specifies a protocol carried over IPv4 by its number in the range of 0 to 255 or by its keyword, as shown in Table 6.

Table 6 Protocols carried over IPv4

Number	Keyword	Description
N/A	**ip**	Matches IPv4 packets.
1	**icmp**	Matches ICMP packets.
2	**igmp**	Matches IGMP packets.
4	**ipinip**	Matches IP-in-IP packets.
6	**tcp**	Matches TCP packets.
17	**udp**	Matches UDP packets.
89	**ospf**	Matches OSPF packets.

Table 7 describes the parameters that you can specify, regardless of the value for the *protocol* argument.

Table 7 Match criteria and other rule information for IPv4 advanced ACL rules

Parameters	Function	Description
source { *source-address source-wildcard* | **any** }	Specifies a source address.	The *source-address source-wildcard* arguments specify a source IP address and a wildcard mask in dotted decimal notation. An all-zero wildcard represents a host address. The **any** keyword specifies any source IP address.
destination { *dest-address dest-wildcard* | **any** }	Specifies a destination address.	The *dest-address dest-wildcard* arguments specify a destination IP address and a wildcard mask in dotted decimal notation. An all-zero wildcard mask represents a host address. The **any** keyword represents any destination IP address.
counting	Enables rule match counting in software.	The **counting** keyword enables match counting specific to rules, and the **hardware-count** keyword in the **packet-filter** command enables match counting in hardware for all rules in an ACL. If the **counting** keyword is not specified, matches for the rule are not counted in software.
precedence *precedence*	Specifies an IP precedence value.	The *precedence* argument can be a number in the range of 0 to 7, or in words: **routine** (0), **priority** (1), **immediate** (2), **flash** (3), **flash-override** (4), **critical** (5), **internet** (6), or **network** (7).
tos *tos*	Specifies a ToS preference.	The *tos* argument can be a number in the range of 0 to 15, or in words: **max-reliability** (2), **max-throughput** (4), **min-delay** (8), **min-monetary-cost** (1), or **normal** (0).
dscp *dscp*	Specifies a DSCP priority.	The *dscp* argument can be a number in the range of 0 to 63, or in words: **af11** (10), **af12** (12), **af13** (14), **af21** (18), **af22** (20), **af23** (22), **af31** (26), **af32** (28), **af33** (30), **af41** (34), **af42** (36), **af43** (38), **cs1** (8), **cs2** (16), **cs3** (24), **cs4** (32), **cs5** (40), **cs6** (48), **cs7** (56), **default** (0), or **ef** (46).
fragment	Applies the rule only to fragments.	If you do not specify this keyword, the rule applies to all fragments and non-fragments.
logging	Logs the number of matching packets.	This feature requires that the module (for example, packet filtering) that uses the ACL supports logging.
time-range *time-range-name*	Specifies a time range for the rule.	The *time-range-name* argument is a case-insensitive string of 1 to 32

		characters. It must start with an English letter. If the time range is not configured, the system creates the rule. However, the rule using the time range can take effect only after you configure the time range. For more information about time range, see *ACL and QoS Configuration Guide*.

If the *protocol* argument is **tcp** (6) or **udp** (17), set the parameters shown in Table 8.

Table 8 TCP/UDP-specific parameters for IPv4 advanced ACL rules

Parameters	Function	Description
source-port *operator port*	Specifies a UDP or TCP source port.	The *operator* argument can be **lt** (lower than), **gt** (greater than), **eq** (equal to), or **range** (inclusive range). The *port1* and *port2* arguments are TCP or UDP port numbers in the range of 0 to 65535. The *port2* argument is needed only when the *operator* argument is **range**. The **lt**, **gt**, and **range** values are supported only in Release 6320 and later.
destination-port *operator port*	Specifies a UDP or TCP destination port.	TCP port numbers can be represented as: **chargen** (19), **bgp** (179), **cmd** (514), **daytime** (13), **discard** (9), **dns** (53), **domain** (53), **echo** (7), **exec** (512), **finger** (79), **ftp** (21), **ftp-data** (20), **gopher** (70), **hostname** (101), **irc** (194), **klogin** (543), **kshell** (544), **login** (513), **lpd** (515), **nntp** (119), **pop2** (109), **pop3** (110), **smtp** (25), **sunrpc** (111), **tacacs** (49), **talk** (517), **telnet** (23), **time** (37), **uucp** (540), **whois** (43), and **www** (80). UDP port numbers can be represented as: **biff** (512), **bootpc** (68), **bootps** (67), **discard** (9), **dns** (53), **dnsix** (90), **echo** (7), **mobilip-ag** (434), **mobilip-mn** (435), **nameserver** (42), **netbios-dgm** (138), **netbios-ns** (137), **netbios-ssn** (139), **ntp** (123), **rip** (520), **snmp** (161), **snmptrap** (162), **sunrpc** (111), **syslog** (514), **tacacs-ds** (65), **talk** (517), **tftp** (69), **time** (37), **who** (513), and **xdmcp** (177).
{ **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } *	Specifies one or more TCP flags including ACK, FIN, PSH, RST, SYN, and URG.	Parameters specific to TCP. The value for each argument can be 0 (flag bit not set) or 1 (flag bit set). The TCP flags in a rule are ANDed. For example, a rule configured with **ack** 0 **psh** 1 matches packets that have the ACK flag bit not set and the PSH flag bit set.
established	Specifies the flags for indicating the established status of a TCP connection.	Parameter specific to TCP. The rule matches TCP connection packets with the ACK or RST flag bit set.

If the *protocol* argument is **icmp** (1), set the parameters shown in Table 9.

Table 9 ICMP-specific parameters for IPv4 advanced ACL rules

Parameters	Function	Description
icmp-type { *icmp-type* *icmp-code* | *icmp-message* }	Specifies the ICMP message type and code.	The *icmp-type* argument is in the range of 0 to 255. The *icmp-code* argument is in the range of 0 to 255. The *icmp-message* argument specifies a message name. Supported ICMP message names and their corresponding type and code values are listed in Table 10.

Table 10 ICMP message names supported in IPv4 advanced ACL rules

ICMP message name	ICMP message type	ICMP message code
echo	8	0
echo-reply	0	0
fragmentneed-DFset	3	4
host-redirect	5	1
host-tos-redirect	5	3
host-unreachable	3	1
information-reply	16	0
information-request	15	0
net-redirect	5	0
net-tos-redirect	5	2
net-unreachable	3	0
parameter-problem	12	0
port-unreachable	3	3
protocol-unreachable	3	2
reassembly-timeout	11	1
source-quench	4	0
source-route-failed	3	5
timestamp-reply	14	0
timestamp-request	13	0
ttl-exceeded	11	0

Usage guidelines

Within an ACL, the permit or deny statement of each rule must be unique. If the rule you are creating or editing has the same deny or permit statement as another rule in the ACL, the rule will not be created or changed.

You can edit ACL rules only when the match order is **config**.

To view the existing IPv4 basic and advanced ACL rules, use the **display acl all** command.

The **undo rule** *rule-id* command without any optional parameters deletes an entire rule. If you specify optional parameters, the **undo rule** *rule-id* command deletes the specified attributes for the rule.

The **undo rule** { **deny** | **permit** } command can only be used to delete an entire rule. You must specify all the attributes of the rule for the command.

Examples

Create an IPv4 advanced ACL rule to permit TCP packets with the destination port 80 from 129.9.0.0/16 to 202.38.160.0/24.

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule permit tcp source 129.9.0.0 0.0.255.255 destination
202.38.160.0 0.0.0.255 destination-port eq 80
```

Create IPv4 advanced ACL rules to permit all IP packets but the ICMP packets destined for 192.168.1.0/24.

```
<Sysname> system-view
[Sysname] acl advanced 3001
[Sysname-acl-ipv4-adv-3001] rule deny icmp destination 192.168.1.0 0.0.0.255
[Sysname-acl-ipv4-adv-3001] rule permit ip
```

Create IPv4 advanced ACL rules to permit inbound and outbound FTP packets.

```
<Sysname> system-view
[Sysname] acl advanced 3002
[Sysname-acl-ipv4-adv-3002] rule permit tcp source-port eq ftp
[Sysname-acl-ipv4-adv-3002] rule permit tcp source-port eq ftp-data
[Sysname-acl-ipv4-adv-3002] rule permit tcp destination-port eq ftp
[Sysname-acl-ipv4-adv-3002] rule permit tcp destination-port eq ftp-data
```

Create IPv4 advanced ACL rules to permit inbound and outbound SNMP and SNMP trap packets.

```
<Sysname> system-view
[Sysname] acl advanced 3003
[Sysname-acl-ipv4-adv-3003] rule permit udp source-port eq snmp
[Sysname-acl-ipv4-adv-3003] rule permit udp source-port eq snmptrap
[Sysname-acl-ipv4-adv-3003] rule permit udp destination-port eq snmp
[Sysname-acl-ipv4-adv-3003] rule permit udp destination-port eq snmptrap
```

Related commands

acl

acl logging interval

display acl

step

time-range

rule (IPv4 basic ACL view)

Use **rule** to create or edit an IPv4 basic ACL rule.

Use **undo rule** to delete an entire IPv4 basic ACL rule or some attributes in the rule.

Syntax

rule [*rule-id*] { **deny** | **permit** } [**counting** | **fragment** | **logging** | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-range-name*] *

undo rule *rule-id* [**counting** | **fragment** | **logging** | **source** | **time-range**] *

undo rule { **deny** | **permit** } [**counting** | **fragment** | **logging** | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-range-name*] *

Default

No IPv4 basic ACL rules exist.

Views

IPv4 basic ACL view

Predefined user roles

network-admin

Parameters

rule-id: Specifies a rule ID in the range of 0 to 65534. If you do not specify a rule ID when creating an ACL rule, the system automatically assigns it a rule ID. This rule ID is the nearest higher multiple of the numbering step to the current highest rule ID, starting from the start rule ID. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the rule is numbered 30.

deny: Denies matching packets.

permit: Allows matching packets to pass.

counting: Enables rule match counting in software. If you do not specify this keyword, matches for the rule are not counted in software.

fragment: Applies the rule only to fragments. If you do not specify this keyword, the rule applies to both fragments and non-fragments.

logging: Logs the number of matching packets. This feature is available only when the application module (for example, packet filtering) that uses the ACL supports the logging feature.

source { *source-address source-wildcard* | **any** }: Matches a source address. The *source-address* and *source-wildcard* arguments specify a source IP address and a wildcard mask in dotted decimal notation. A wildcard mask of zeros represents a host address. The **any** keyword represents any source IP address.

time-range *time-range-name*: Specifies a time range for the rule. The *time-range-name* argument is a case-insensitive string of 1 to 32 characters. It must start with an English letter. If the time range is not configured, the system creates the rule. However, the rule using the time range can take effect only after you configure the time range. For more information about time range, see *ACL and QoS Configuration Guide*.

Usage guidelines

Within an ACL, the permit or deny statement of each rule must be unique. If the rule you are creating or editing has the same deny or permit statement as another rule in the ACL, the rule will not be created or changed.

You can edit ACL rules only when the match order is **config**.

The **counting** keyword in this command enables match counting specific to rules, and the **hardware-count** keyword in the **packet-filter** command enables match counting in hardware for all rules in an ACL.

To view the existing IPv4 basic and advanced ACL rules, use the **display acl all** command.

The **undo rule** *rule-id* command without any optional parameters deletes an entire rule. If you specify optional parameters, the **undo rule** *rule-id* command deletes the specified attributes for the rule.

The **undo rule** { **deny** | **permit** } command can only be used to delete an entire rule. You must specify all the attributes of the rule for the command.

Examples

Create a rule in IPv4 basic ACL 2000 to deny the packets from any source IP subnet but 10.0.0.0/8, 172.17.0.0/16, or 192.168.1.0/24.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule permit source 10.0.0.0 0.255.255.255
[Sysname-acl-ipv4-basic-2000] rule permit source 172.17.0.0 0.0.255.255
[Sysname-acl-ipv4-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Sysname-acl-ipv4-basic-2000] rule deny source any
```

Related commands

acl

acl logging interval

display acl

step

time-range

rule (IPv6 advanced ACL view)

Use **rule** to create or edit an IPv6 advanced ACL rule.

Use **undo rule** to delete an entire IPv6 advanced ACL rule or some attributes in the rule.

Syntax

rule [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { *dest-address dest-prefix* | *dest-address/dest-prefix* | **any** } | **destination-port** *operator port* | **dscp** *dscp* | **flow-label** *flow-label-value* | **fragment** | **icmp6-type** { *icmp6-type icmp6-code* | *icmp6-message* } | **logging** | **routing** [**type** *routing-type*] | **hop-by-hop** [**type** *hop-type*] | **source** { *source-address source-prefix* | *source-address/source-prefix* | **any** } | **source-port** *operator port* | **time-range** *time-range-name*] *

undo rule *rule-id* [{ { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **established** } | **counting** | **destination** | **destination-port** | **dscp** | **flow-label** | **fragment** | **icmp6-type** | **logging** | **routing** | **hop-by-hop** | **source** | **source-port** | **time-range**] *

undo rule { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { *dest-address dest-prefix* | *dest-address/dest-prefix* | **any** } | **destination-port** *operator port* | **dscp** *dscp* | **flow-label** *flow-label-value* | **fragment** | **icmp6-type** { *icmp6-type icmp6-code* | *icmp6-message* } | **logging** | **routing** [**type** *routing-type*] | **hop-by-hop** [**type** *hop-type*] | **source** { *source-address source-prefix* | *source-address/source-prefix* | **any** } | **source-port** *operator port* | **time-range** *time-range-name*] *

Default

No IPv6 advanced ACL rules exist.

Views

IPv6 advanced ACL view

Predefined user roles

network-admin

Parameters

rule-id: Specifies a rule ID in the range of 0 to 65534. If you do not specify a rule ID when creating an ACL rule, the system automatically assigns it a rule ID. This rule ID is the nearest higher multiple of the numbering step to the current highest rule ID, starting from the start rule ID. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the rule is numbered 30.

deny: Denies matching packets.

permit: Allows matching packets to pass.

protocol: Specifies a protocol carried over IPv6 by its number in the range of 0 to 255 or by its keyword, as shown in Table 11.

Table 11 Protocols carried over IPv6

Number	Keyword	Description
N/A	**ipv6**	Matches IPv6 packets.
1	**icmpv6**	Matches ICMPv6 packets.
6	**tcp**	Matches TCP packets.
17	**udp**	Matches UDP packets.
50	**ipv6-esp**	Matches IPv6-ESP packets.
51	**ipv6-ah**	Matches IPv6-AH packets.
89	**ospf**	Matches OSPF packets.

Table 12 describes the parameters that you can specify, regardless of the value for the *protocol* argument.

Table 12 Match criteria and other rule information for IPv6 advanced ACL rules

Parameters	Function	Description
source { *source-address source-prefix* | *source-address/source-prefix* | **any** }	Specifies a source IPv6 address.	The *source-address* argument specifies an IPv6 source address. The *source-prefix* argument specifies a prefix length in the range of 1 to 128. The **any** keyword represents any IPv6 source address.
destination { *dest-address dest-prefix* | *dest-address/dest-prefix* | **any** }	Specifies a destination IPv6 address.	The *dest-address* argument specifies a destination IPv6 address. The *dest-prefix* argument specifies a prefix length in the range of 1 to 128. The **any** keyword represents any IPv6 destination address.
counting	Enables rule match counting in software.	The **counting** keyword enables match counting specific to rules, and the **hardware-count** keyword in the **packet-filter ipv6** command enables match counting in hardware for all rules in an ACL. If the **counting** keyword is not specified,

		matches for the rule are not counted in software.
dscp *dscp*	Specifies a DSCP preference.	The *dscp* argument can be a number in the range of 0 to 63, or in words, **af11** (10), **af12** (12), **af13** (14), **af21** (18), **af22** (20), **af23** (22), **af31** (26), **af32** (28), **af33** (30), **af41** (34), **af42** (36), **af43** (38), **cs1** (8), **cs2** (16), **cs3** (24), **cs4** (32), **cs5** (40), **cs6** (48), **cs7** (56), **default** (0), or **ef** (46).
flow-label *flow-label-value*	Specifies a flow label value in an IPv6 packet header.	The *flow-label-value* argument is in the range of 0 to 1048575.
fragment	Applies the rule only to fragments.	If you do not specify this keyword, the rule applies to all fragments and non-fragments.
logging	Logs the number of matching packets.	This feature requires that the module (for example, packet filtering) that uses the ACL supports logging.
routing [**type** *routing-type*]	Specifies an IPv6 routing header type.	*routing-type*: Value of the IPv6 routing header type, in the range of 0 to 255. If you specify the **type** *routing-type* option, the rule applies to the specified type of IPv6 routing header. If you do not specify the **type** *routing-type* option, the rule applies to all types of IPv6 routing headers.
hop-by-hop [**type** *hop-type*]	Specifies an IPv6 Hop-by-Hop Options header type.	*hop-type*: Value of the IPv6 Hop-by-Hop Options header type, in the range of 0 to 255. If you specify the **type** *hop-type* option, the rule applies to the specified type of IPv6 Hop-by-Hop Options header. If you do not specify the **type** *hop-type* option, the rule applies to all types of IPv6 Hop-by-Hop Options header.
time-range *time-range-name*	Specifies a time range for the rule.	The *time-range-name* argument is a case-insensitive string of 1 to 32 characters. It must start with an English letter. If the time range is not configured, the system creates the rule. However, the rule using the time range can take effect only after you configure the time range. For more information about time range, see *ACL and QoS Configuration Guide*.

If the *protocol* argument is **tcp** (6) or **udp** (17), set the parameters shown in Table 13.

Table 13 TCP/UDP-specific parameters for IPv6 advanced ACL rules

Parameters	Function	Description
source-port *operator port*	Specifies a UDP or TCP source port.	The *operator* argument can be **lt** (lower than), **gt** (greater than), **eq** (equal to), or **range** (inclusive range). The *port1* and *port2* arguments are TCP or UDP port numbers in the range of 0 to 65535. The *port2* argument is needed only when the *operator* argument is **range**. The **lt**, **gt**, and **range** values are supported only in Release 6320 and later.
destination-port *operator port*	Specifies a UDP or TCP destination port.	

		TCP port numbers can be represented as: **chargen** (19), **bgp** (179), **cmd** (514), **daytime** (13), **discard** (9), **dns** (53), **domain** (53), **echo** (7), **exec** (512), **finger** (79), **ftp** (21), **ftp-data** (20), **gopher** (70), **hostname** (101), **irc** (194), **klogin** (543), **kshell** (544), **login** (513), **lpd** (515), **nntp** (119), **pop2** (109), **pop3** (110), **smtp** (25), **sunrpc** (111), **tacacs** (49), **talk** (517), **telnet** (23), **time** (37), **uucp** (540), **whois** (43), and **www** (80). UDP port numbers can be represented as: **biff** (512), **bootpc** (68), **bootps** (67), **discard** (9), **dns** (53), **dnsix** (90), **echo** (7), **mobilip-ag** (434), **mobilip-mn** (435), **nameserver** (42), **netbios-dgm** (138), **netbios-ns** (137), **netbios-ssn** (139), **ntp** (123), **rip** (520), **snmp** (161), **snmptrap** (162), **sunrpc** (111), **syslog** (514), **tacacs-ds** (65), **talk** (517), **tftp** (69), **time** (37), **who** (513), and **xdmcp** (177).
{ **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* }*	Specifies one or more TCP flags, including ACK, FIN, PSH, RST, SYN, and URG.	Parameters specific to TCP. The value for each argument can be 0 (flag bit not set) or 1 (flag bit set). The TCP flags in a rule are ANDed. For example, a rule configured with **ack** 0 **psh** 1 matches packets that have the ACK flag bit not set and the PSH flag bit set.
established	Specifies the flags for indicating the established status of a TCP connection.	Parameter specific to TCP. The rule matches TCP packets with the ACK or RST flag bit set.

If the *protocol* argument is **icmpv6** (58), set the parameters shown in Table 14.

Table 14 ICMPv6-specific parameters for IPv6 advanced ACL rules

Parameters	Function	Description
icmp6-type { *icmp6-type icmp6-code* | *icmp6-message* }	Specifies the ICMPv6 message type and code.	The *icmp6-type* argument is in the range of 0 to 255. The *icmp6-code* argument is in the range of 0 to 255. The *icmp6-message* argument specifies a message name. Supported ICMP message names and their corresponding type and code values are listed in Table 15.

Table 15 ICMPv6 message names supported in IPv6 advanced ACL rules

ICMPv6 message name	ICMPv6 message type	ICMPv6 message code
echo-reply	129	0
echo-request	128	0
err-Header-field	4	0
frag-time-exceeded	3	1
hop-limit-exceeded	3	0
host-admin-prohib	1	1
host-unreachable	1	3
neighbor-advertisement	136	0
neighbor-solicitation	135	0

network-unreachable	1	0
packet-too-big	2	0
port-unreachable	1	4
redirect	137	0
router-advertisement	134	0
router-solicitation	133	0
unknown-ipv6-opt	4	2
unknown-next-hdr	4	1

Usage guidelines

If an IPv6 advanced ACL is for QoS traffic classification or packet filtering:

- Do not specify the **fragment** keyword.
- Do not specify the **routing**, **hop-by-hop**, or **flow-label** keyword if the ACL is for outbound application.

Within an ACL, the permit or deny statement of each rule must be unique. If the rule you are creating or editing has the same deny or permit statement as another rule in the ACL, the rule will not be created or changed.

You can edit ACL rules only when the match order is **config**.

To view the existing IPv6 basic and advanced ACL rules, use the **display acl ipv6 all** command.

The **undo rule** *rule-id* command without any optional parameters deletes an entire rule. If you specify optional parameters, the **undo rule** *rule-id* command deletes the specified attributes for a rule.

The **undo rule** { **deny** | **permit** } command can only be used to delete an entire rule. You must specify all the attributes of the rule for the command.

Examples

Create an IPv6 advanced ACL rule to permit TCP packets with the destination port 80 from 2030:5060::/64 to FE80:5060::/96.

```
<Sysname> system-view
[Sysname] acl ipv6 advanced 3000
[Sysname-acl-ipv6-adv-3000] rule permit tcp source 2030:5060::/64 destination
fe80:5060::/96 destination-port eq 80
```

Create IPv6 advanced ACL rules to permit all IPv6 packets but the ICMPv6 packets destined for FE80:5060:1001::/48.

```
<Sysname> system-view
[Sysname] acl ipv6 advanced 3001
[Sysname-acl-ipv6-adv-3001] rule deny icmpv6 destination fe80:5060:1001:: 48
[Sysname-acl-ipv6-adv-3001] rule permit ipv6
```

Create IPv6 advanced ACL rules to permit inbound and outbound FTP packets.

```
<Sysname> system-view
[Sysname] acl ipv6 advanced 3002
[Sysname-acl-ipv6-adv-3002] rule permit tcp source-port eq ftp
[Sysname-acl-ipv6-adv-3002] rule permit tcp source-port eq ftp-data
[Sysname-acl-ipv6-adv-3002] rule permit tcp destination-port eq ftp
[Sysname-acl-ipv6-adv-3002] rule permit tcp destination-port eq ftp-data
```

Create IPv6 advanced ACL rules to permit inbound and outbound SNMP and SNMP trap packets.

```
<Sysname> system-view
[Sysname] acl ipv6 advanced 3003
[Sysname-acl-ipv6-adv-3003] rule permit udp source-port eq snmp
[Sysname-acl-ipv6-adv-3003] rule permit udp source-port eq snmptrap
[Sysname-acl-ipv6-adv-3003] rule permit udp destination-port eq snmp
[Sysname-acl-ipv6-adv-3003] rule permit udp destination-port eq snmptrap
```

Create IPv6 advanced ACL 3004, and configure two rules: one permits packets with the Hop-by-Hop Options header type as 5, and the other one denies packets with other Hop-by-Hop Options header types.

```
<Sysname> system-view
[Sysname] acl ipv6 advanced 3004
[Sysname-acl-ipv6-adv-3004] rule permit ipv6 hop-by-hop type 5
[Sysname-acl-ipv6-adv-3004] rule deny ipv6 hop-by-hop
```

Related commands

acl

acl logging interval

display acl

step

time-range

rule (IPv6 basic ACL view)

Use **rule** to create or edit an IPv6 basic ACL rule.

Use **undo rule** to delete an entire IPv6 basic ACL rule or some attributes in the rule.

Syntax

rule [*rule-id*] { **deny** | **permit** } [**counting** | **fragment** | **logging** | **routing** [**type** *routing-type*] | **source** { *source-address source-prefix* | *source-address*/*source-prefix* | **any** } | **time-range** *time-range-name*] *

undo rule *rule-id* [**counting** | **fragment** | **logging** | **routing** | **source** | **time-range**] *

undo rule { **deny** | **permit** } [**counting** | **fragment** | **logging** | **routing** [**type** *routing-type*] | **source** { *source-address source-prefix* | *source-address*/*source-prefix* | **any** } | **time-range** *time-range-name*] *

Default

No IPv6 basic ACL rules exist.

Views

IPv6 basic ACL view

Predefined user roles

network-admin

Parameters

rule-id: Specifies a rule ID in the range of 0 to 65534. If you do not specify a rule ID when creating an ACL rule, the system automatically assigns it a rule ID. This rule ID is the nearest higher multiple

of the numbering step to the current highest rule ID, starting from the start rule ID. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the rule is numbered 30.

deny: Denies matching packets.

permit: Allows matching packets to pass.

counting: Enables rule match counting in software. If you do not specify this keyword, matches for the rule are not counted in software.

fragment: Applies the rule only to fragments. If you do not specify this keyword, the rule applies to both fragments and non-fragments.

logging: Logs the number of matching packets. This feature is available only when the application module (for example, packet filtering) that uses the ACL supports the logging feature.

routing [**type** *routing-type*]: Applies the rule to the specified type of IPv6 routing header or all types of IPv6 routing headers. The *routing-type* argument specifies the value of the IPv6 routing header type, in the range of 0 to 255. If you do not specify the **type** *routing-type* option, the rule applies to all types of IPv6 routing headers.

source { *source-address source-prefix* | *source-address*/*source-prefix* | **any** }: Matches a source IPv6 address. The *source-address* argument specifies a source IPv6 address. The *source-prefix* argument specifies an address prefix length in the range of 1 to 128. The **any** keyword represents any IPv6 source address.

time-range *time-range-name*: Specifies a time range for the rule. The *time-range-name* argument is a case-insensitive string of 1 to 32 characters. It must start with an English letter. If the time range is not configured, the system creates the rule. However, the rule using the time range can take effect only after you configure the time range. For more information about time range, see *ACL and QoS Configuration Guide*.

Usage guidelines

The **fragment** keyword is not supported for a QoS policy or a packet filter.

The **routing** keyword is not supported for an outbound QoS policy or packet filter.

Within an ACL, the permit or deny statement of each rule must be unique. If the rule you are creating or editing has the same deny or permit statement as another rule in the ACL, the rule will not be created or changed.

You can edit ACL rules only when the match order is **config**.

The **counting** keyword in this command enables match counting specific to rules, and the **hardware-count** keyword in the **packet-filter ipv6** command enables match counting in hardware for all rules in an ACL.

To view the existing IPv6 basic and advanced ACL rules, use the **display acl ipv6 all** command.

The **undo rule** *rule-id* command without any optional parameters deletes an entire rule. If you specify optional parameters, the **undo rule** *rule-id* command deletes the specified attributes for a rule.

The **undo rule** { **deny** | **permit** } command can only be used to delete an entire rule. You must specify all the attributes of the rule for the command.

Examples

Create an IPv6 basic ACL rule to deny the packets from any source IP subnet but 1001::/16, 3124:1123::/32, or FE80:5060:1001::/48.

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2000
[Sysname-acl-ipv6-basic-2000] rule permit source 1001:: 16
```

```
[Sysname-acl-ipv6-basic-2000] rule permit source 3124:1123:: 32
[Sysname-acl-ipv6-basic-2000] rule permit source fe80:5060:1001:: 48
[Sysname-acl-ipv6-basic-2000] rule deny source any
```

Related commands

acl

acl logging interval

display acl

step

time-range

rule (Layer 2 ACL view)

Use **rule** to create or edit a Layer 2 ACL rule.

Use **undo rule** to delete an entire Layer 2 ACL rule or some attributes in the rule.

Syntax

rule [*rule-id*] { **deny** | **permit** } [**cos** *dot1p* | **counting** | **dest-mac** *dest-address dest-mask* | { **lsap** *lsap-type lsap-type-mask* | **type** *protocol-type protocol-type-mask* } | **source-mac** *source-address source-mask* | **time-range** *time-range-name*] *

undo rule *rule-id* [**counting** | **time-range**] *

undo rule { **deny** | **permit** } [**cos** *dot1p* | **counting** | **dest-mac** *dest-address dest-mask* | { **lsap** *lsap-type lsap-type-mask* | **type** *protocol-type protocol-type-mask* } | **source-mac** *source-address source-mask* | **time-range** *time-range-name*] *

Default

No Layer 2 ACL rules exist.

Views

Layer 2 ACL view

Predefined user roles

network-admin

Parameters

rule-id: Specifies a rule ID in the range of 0 to 65534. If you do not specify a rule ID when creating an ACL rule, the system automatically assigns it a rule ID. This rule ID is the nearest higher multiple of the numbering step to the current highest rule ID, starting from the start rule ID. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the rule is numbered 30.

deny: Denies matching packets.

permit: Allows matching packets to pass.

cos *dot1p:* Matches an 802.1p priority. The 802.1p priority can be specified by one of the following values:

- A priority number in the range of 0 to 7.
- A priority name: **best-effort** (0), **background** (1), **spare** (2), **excellent-effort** (3), **controlled-load** (4), **video** (5), **voice** (6), or **network-management** (7).

counting: Enables rule match counting in software. If you do not specify this keyword, matches for the rule are not counted in software.

dest-mac *dest-address dest-mask:* Matches a destination MAC address range. The *dest-address* and *dest-mask* arguments represent a destination MAC address and mask in the H-H-H format.

lsap *lsap-type lsap-type-mask:* Matches the DSAP and SSAP fields in LLC encapsulation. The *lsap-type* argument is a hexadecimal number that represents the encapsulation format. The value range for the *lsap-type* argument is 0 to ffff. The *lsap-type-mask* argument is a hexadecimal number that represents the LSAP mask. The value range for the *lsap-type-mask* argument is 0 to ffff.

type *protocol-type protocol-type-mask*: Matches one or more protocols in the Layer 2. The *protocol-type* argument is a hexadecimal number that represents a protocol type in Ethernet_II and Ethernet_SNAP frames. The value range for the *protocol-type* argument is 0 to ffff. The *protocol-type-mask* argument is a hexadecimal number that represents a protocol type mask. The value range for the *protocol-type-mask* argument is 0 to ffff.

source-mac *source-address source-mask:* Matches a source MAC address range. The *source-address* argument represents a source MAC address, and the *sour-mask* argument represents a mask in the H-H-H format.

time-range *time-range-name*: Specifies a time range for the rule. The *time-range-name* argument is a case-insensitive string of 1 to 32 characters. It must start with an English letter. If the time range is not configured, the system creates the rule. However, the rule using the time range can take effect only after you configure the time range. For more information about time range, see *ACL and QoS Configuration Guide*.

Usage guidelines

Within an ACL, the permit or deny statement of each rule must be unique. If the rule you are creating or editing has the same deny or permit statement as another rule in the ACL, the rule will not be created or changed.

You can edit ACL rules only when the match order is **config**.

The **counting** keyword in this command enables match counting specific to rules, and the **hardware-count** keyword in the **packet-filter** command enables match counting in hardware for all rules in an ACL.

To view the existing Layer 2 ACL rules, use the **display acl mac all** command.

The **undo rule** *rule-id* command without any optional parameters deletes an entire rule. If you specify optional parameters, the **undo rule** *rule-id* command deletes the specified attributes for the rule.

The **undo rule** { **deny** | **permit** } command can only be used to delete an entire rule. You must specify all the attributes of the rule for the command.

Examples

Create a rule in Layer 2 ACL 4000 to permit ARP packets and deny RARP packets.

```
<Sysname> system-view
[Sysname] acl mac 4000
[Sysname-acl-mac-4000] rule permit type 0806 ffff
[Sysname-acl-mac-4000] rule deny type 8035 ffff
```

Related commands

acl

display acl

step

time-range

rule comment

Use **rule comment** to configure a comment for an ACL rule.

Use **undo rule comment** to delete an ACL rule comment.

Syntax

rule *rule-id* **comment** *text*

undo rule *rule-id* **comment**

Default

A rule does not have a comment.

Views

IPv4 basic/advanced ACL view

IPv6 basic/advanced ACL view

Layer 2 ACL view

Predefined user roles

network-admin

Parameters

rule-id: Specifies an ACL rule ID in the range of 0 to 65534. The ACL rule must already exist.

text: Specifies a comment about the ACL rule, a case-sensitive string of 1 to 127 characters.

Usage guidelines

This command adds a comment to a rule if the rule does not have a comment. It modifies the comment for a rule if the rule already has a comment.

Examples

Create a rule for IPv4 basic ACL 2000, and add a comment about the rule.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule 0 deny source 1.1.1.1 0
[Sysname-acl-ipv4-basic-2000] rule 0 comment This rule is used on gigabitethernet 1/0/1.
```

Related commands

display acl

step

Use **step** to set a rule numbering step for an ACL.

Use **undo step** to restore the default.

Syntax

step *step-value* [**start** *start-value*]

undo step

Default

The rule numbering step is 5, and the start rule ID is 0.

Views

IPv4 basic/advanced ACL view

IPv6 basic/advanced ACL view

Layer 2 ACL view

Predefined user roles

network-admin

Parameters

step-value: Specifies the ACL rule numbering step in the range of 1 to 20.

start *start-value*: Specifies the start rule ID in the range of 0 to 20.

Usage guidelines

The rule numbering step sets the increment by which the system numbers rules automatically. If you do not specify a rule ID when creating an ACL rule, the system automatically assigns it a rule ID. This rule ID is the nearest higher multiple of the numbering step to the current highest rule ID, starting from the start rule ID. For example, if the rule numbering step is 5 and the current highest rule ID is 12, the rule is numbered 15.

The wider the numbering step, the more rules you can insert between two rules. Whenever the step or start rule ID changes, the rules are renumbered, starting from the start rule ID. For example, if there are five rules numbered 0, 5, 9, 10, and 15, changing the step from 5 to 2 causes the rules to be renumbered 0, 2, 4, 6, and 8.

Examples

Set the rule numbering step to 2 for IPv4 basic ACL 2000.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] step 2
```

Related commands

display acl

Contents

QoS policy commands

Traffic class commands

description

Use **description** to configure a description for a traffic class.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

No description is configured for a traffic class.

Views

Traffic class view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 127 characters.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure the description as **classifier** for traffic class **class1**.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] description classifier
```

display traffic classifier

Use **display traffic classifier** to display traffic classes.

Syntax

display traffic classifier user-defined [*classifier-name*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

user-defined: Specifies user-defined traffic classes.

classifier-name: Specifies a traffic class by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a traffic class, this command displays all traffic classes.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the traffic classes for the master device.

Examples

Display all user-defined traffic classes.

```
<Sysname> display traffic classifier user-defined

  User-defined classifier information:

   Classifier: 1 (ID 100)
     Operator: AND
     Rule(s) :
      If-match acl 2000

   Classifier: 2 (ID 101)
     Operator: AND
     Rule(s) :
      If-match protocol ipv6

   Classifier: 3 (ID 102)
     Operator: AND
     Rule(s) :
      -none-
```

Table 1 Command output

Field	Description
Classifier	Traffic class name and its match criteria.
Operator	Match operator you set for the traffic class. If the operator is AND, the traffic class matches the packets that match all its match criteria. If the operator is OR, the traffic class matches the packets that match any of its match criteria.
Rule(s)	Match criteria.

if-match

Use **if-match** to define a match criterion.

Use **undo if-match** to delete a match criterion.

Syntax

if-match *match-criteria*

undo if-match *match-criteria*

Default

No match criterion is configured.

Views

Traffic class view

Predefined user roles

network-admin

Parameters

match-criteria: Specifies a match criterion. Table 2 shows the available match criteria.

Table 2 Available match criteria

Option	Description
acl [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }	Matches an ACL. The value range for the *acl-number* argument is as follows: • 2000 to 3999 for IPv4 ACLs. • 2000 to 3999 for IPv6 ACLs. • 4000 to 4999 for Layer 2 MAC ACLs. The *acl-name* argument is a case-insensitive string of 1 to 63 characters, which must start with an English letter. To avoid confusion, make sure the argument is not **all**.
any	Matches all packets.
customer-vlan-id *vlan-id-list*	Matches VLAN IDs in inner VLAN tags of double-tagged packets. The *vlan-id-list* argument specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* **to** *vlan-id2*. The value for *vlan-id2* must be greater than or equal to the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094. The **if-match customer-vlan-id** *vlan-id-list* command can only be used to match single-tagged packets for the nesting (outer VLAN tag adding) action,
destination-mac *mac-address* [*mac-address-mask*]	Matches a destination MAC address. This option takes effect only on Ethernet interfaces.
dscp *dscp-value*&<1-8>	Matches DSCP values. The *dscp-value*&<1-8> argument specifies a space-separated list of up to eight DSCP values. The value range for the *dscp-value* argument is 0 to 63 or keywords shown in Table 4.
ip-precedence *ip-precedence-value*&<1-8>	Matches IP precedence values. The *ip-precedence-value*&<1-8> argument specifies a space-separated list of up to eight IP precedence values. The value range for the *ip-precedence-value* argument is 0 to 7.
protocol *protocol-name*	Matches a protocol. The *protocol-name* argument can be **ip** or **ipv6**.

Option	Description
service-dot1p *dot1p-value*&<1-8>	Matches 802.1p priority values in outer VLAN tags. The *dot1p-value*&<1-8> argument specifies a space-separated list of up to eight 802.1p priority values. The value range for the *dot1p-value* argument is 0 to 7.
service-vlan-id *vlan-id-list*	Matches VLAN IDs in outer VLAN tags. The *vlan-id-list* argument specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of *vlan-id1* **to** *vlan-id2*. The value for *vlan-id2* must be greater than or equal to the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094. You can use this option to match single-tagged packets typically except for the nesting (outer VLAN tag adding) action.
source-mac *mac-address* [*mac-address-mask*]	Matches a source MAC address. This option takes effect only on Ethernet interfaces.

Usage guidelines

In a traffic class with the logical OR operator, you can configure multiple **if-match** commands for any of the available match criteria.

When you configure a match criterion that can have multiple values in one **if-match** command, follow these restrictions and guidelines:

- You can specify up to eight values for any of the following match criteria in one **if-match** command:
  - 802.1p priority.
  - DSCP.
  - VLAN ID.
- If a packet matches one of the specified values, it matches the **if-match** command.
- To delete a criterion that has multiple values, the specified values in the **undo if-match** command must be the same as those specified in the **if-match** command. The order of the values can be different.

When you configure ACL-based match criteria, follow these restrictions and guidelines:

- The ACL must already exist.
- The ACL is used for classification only and the permit/deny actions in ACL rules are ignored. Actions taken on matching packets are defined in traffic behaviors.

You can use both AND and OR operators to define the match relationships between the criteria for a class. For example, you can define relationships among three match criteria in traffic class **classA** as follows:

```
traffic classifier classB operator and
if-match criterion 1
if-match criterion 2
traffic classifier classA operator or
if-match criterion 3
```

Examples

Define a match criterion for traffic class **class1** to match the packets with a destination MAC address of 0050-ba27-bed3.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match destination-mac 0050-ba27-bed3
```

Define a match criterion for traffic class **class2** to match the packets with a source MAC address of 0050-ba27-bed2.

```
<Sysname> system-view
[Sysname] traffic classifier class2
[Sysname-classifier-class2] if-match source-mac 0050-ba27-bed2
```

Define a match criterion for traffic class **class1** to match the packets with a source MAC address of 0050-ba27-bed3 and a MAC address mask of ffff-ffff-0000.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match destination-mac 0050-ba27-bed3 ffff-ffff-0000
```

Define a match criterion for traffic class **class2** to match the packets with a source MAC address of 0050-ba27-bed2 and a MAC address mask of ffff-ffff-0000.

```
<Sysname> system-view
[Sysname] traffic classifier class2
[Sysname-classifier-class2] if-match source-mac 0050-ba27-bed2 ffff-ffff-0000
```

Define a match criterion for traffic class **class1** to match the packets with 802.1p priority 5 in the outer VLAN tag.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match service-dot1p 5
```

Define a match criterion for traffic class **class1** to match advanced ACL 3101.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match acl 3101
```

Define a match criterion for traffic class **class1** to match the ACL named **flow**.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match acl name flow
```

Define a match criterion for traffic class **class1** to match advanced IPv6 ACL 3101.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match acl ipv6 3101
```

Define a match criterion for traffic class **class1** to match the IPv6 ACL named **flow**.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match acl ipv6 name flow
```

Define a match criterion for traffic class **class1** to match all packets.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match any
```

Define a match criterion for traffic class **class1** to match the packets with a DSCP value of 1, 6, or 9.

```
<Sysname> system-view
[Sysname] traffic classifier class1 operator or
```

```
[Sysname-classifier-class1] if-match dscp 1 6 9
```

Define a match criterion for traffic class **class1** to match IP packets.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match protocol ip
```

Define a match criterion for traffic class **class1** to match the packets with VLAN ID 2, 7, or 10 in the outer VLAN tag.

```
<Sysname> system-view
[Sysname] traffic classifier class1 operator or
[Sysname-classifier-class1] if-match service-vlan-id 2 7 10
```

traffic classifier

Use **traffic classifier** to create a traffic class and enter its view, or enter the view of an existing traffic class.

Use **undo traffic classifier** to delete a traffic class.

Syntax

traffic classifier *classifier-name* [**operator** { **and** | **or** }]

undo traffic classifier *classifier-name*

Default

No traffic classes exist.

Views

System view

Predefined user roles

network-admin

Parameters

classifier-name: Specifies a name for the traffic class, a case-sensitive string of 1 to 31 characters.

operator: Sets the operator to logic AND (the default) or OR for the traffic class.

and: Specifies the logic AND operator. The traffic class matches the packets that match all its criteria.

or: Specifies the logic OR operator. The traffic class matches the packets that match any of its criteria.

Examples

Create a traffic class named **class1**.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1]
```

Related commands

display traffic classifier

Traffic behavior commands

accounting

Use **accounting** to configure a traffic accounting action in a traffic behavior.

Use **undo accounting** to restore the default.

Syntax

accounting { **byte** | **packet** }

undo accounting

Default

No traffic accounting action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

byte: Counts traffic in bytes.

packet: Counts traffic in packets.

Examples

Configure a traffic accounting action in traffic behavior **database** to count traffic in bytes.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] accounting byte
```

car

Use **car** to configure a CAR action in absolute value in a traffic behavior.

Use **undo car** to restore the default.

Syntax

car cir *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**green** *action* | **red** *action* | **yellow** *action*] *

car cir *committed-information-rate* [**cbs** *committed-burst-size*] **pir** *peak-information-rate* [**ebs** *excess-burst-size*] [**green** *action* | **red** *action* | **yellow** *action*] *

undo car

Default

No CAR action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

cir *committed-information-rate*: Specifies the committed information rate (CIR) in the range of 8 to 160000000 kbps, in increments of 8.

cbs *committed-burst-size*: Specifies the committed burst size (CBS) in bytes. The value range for *committed-burst-size* is 512 to 256000000, in increments of 512. The default value for this argument is the product of 62.5 and the CIR and must be an integral multiple of 512. When the product is not an integral multiple of 512, it is rounded up to the nearest integral multiple of 512 that is greater than the product. A default value greater than 256000000 is converted to 256000000.

ebs *excess-burst-size*: Specifies the excess burst size (EBS) in bytes. The value range for *excess-burst-size* is 0 to 256000000, in increments of 512. If the PIR is configured, the default EBS is the product of 62.5 and the PIR and must be an integral multiple of 512. When the product is not an integral multiple of 512, it is rounded up to the nearest integral multiple of 512. A default value greater than 256000000 is converted to 256000000.

pir *peak-information-rate*: Specifies the peak information rate (PIR) in the range of 8 to 160000000 kbps, in increments of 8.

green *action*: Specifies the action to take on packets that conform to the CIR. The default setting is **pass**.

red *action*: Specifies the action to take on packets that conform to neither CIR nor PIR. The default setting is **discard**.

yellow *action*: Specifies the action to take on packets that conform to the PIR but not to the CIR. The default setting is **pass**.

action: Sets the action to take on the packet:

- **discard**: Drops the packet.
- **pass**: Permits the packet to pass through.
- **remark-dot1p-pass** *new-cos*: Sets the 802.1p priority value of the 802.1p packet to *new-cos* and permits the packet to pass through. The *new-cos* argument is in the range of 0 to 7.
- **remark-dscp-pass** *new-dscp*: Sets the DSCP value of the packet to *new-dscp* and permits the packet to pass through. The *new-dscp* argument is in the range of 0 to 63.
- **remark-lp-pass** *new-local-precedence*: Sets the local precedence value of the packet to *new-local-precedence* and permits the packet to pass through. The *new-local-precedence* argument is in the range of 0 to 7.

Usage guidelines

To use two rates for traffic policing, configure the **car** command with the **pir** *peak-information-rate* option. To use one rate for traffic policing, configure the **car** command without the **pir** *peak-information-rate* option.

If you execute the **car** command multiple times in the same traffic behavior, the most recent configuration takes effect.

Examples

Configure a CAR action in traffic behavior **database**:

- Set the CIR to 200 kbps, CBS to 51200 bytes, and EBS to 0.
- Transmit the conforming packets, and mark the excess packets with DSCP value 0 and transmit them.

```
<Sysname> system-view
```

```
[Sysname] traffic behavior database
[Sysname-behavior-database] car cir 200 cbs 51200 ebs 0 green pass red remark-dscp-pass
0
```

display traffic behavior

Use **display traffic behavior** to display traffic behaviors.

Syntax

display traffic behavior user-defined [*behavior-name*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

user-defined: Specifies user-defined traffic behaviors.

behavior-name: Specifies a behavior by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a traffic behavior, this command displays all traffic behaviors.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the traffic behaviors for the master device.

Examples

Display all user-defined traffic behaviors.

```
<Sysname> display traffic behavior user-defined

  User-defined behavior information:

    Behavior: 1 (ID 100)
      Marking:
        Remark dscp 3
      Committed Access Rate:
        CIR 112 (kbps), CBS 5120 (Bytes), EBS 512 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard

    Behavior: 2 (ID 101)
      Accounting enable: Packet
      Filter enable: Permit
      Redirecting:
        Redirect to the CPU

    Behavior: 3 (ID 102)
      -none-
```

Table 3 Command output

Field	Description
Behavior	Name and contents of a traffic behavior.
Marking	Information about priority marking.
Remark dscp	Action of setting the DSCP value for packets.
Committed Access Rate	Information about the CAR action.
Green action	Action to take on green packets.
Yellow action	Action to take on yellow packets.
Red action	Action to take on red packets.
Accounting enable	Class-based accounting action.
Filter enable	Traffic filtering action.
Redirecting	Information about traffic redirecting.
Mirroring	Information about traffic mirroring.
none	No other traffic behavior is configured.

filter

Use **filter** to configure a traffic filtering action in a traffic behavior.

Use **undo filter** to restore the default.

Syntax

filter { **deny** | **permit** }

undo filter

Default

No traffic filtering action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

deny: Drops packets.

permit: Transmits packets. The permitted packets can be processed by other class-behavior associations in the same QoS policy.

Examples

Configure a traffic filtering action as **deny** in traffic behavior **database**.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] filter deny
```

nest top-most

Use **nest top-most** to configure an outer VLAN tag adding action in a traffic behavior.

Use **undo nest top-most** to restore the default.

Syntax

nest top-most vlan *vlan-id*

undo nest top-most

Default

No outer VLAN tag adding action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

vlan-id *vlan-id*: Specifies the VLAN ID to be added in the outer VLAN tag, in the range of 1 to 4094.

Usage guidelines

If a QoS policy contains an outer VLAN tag adding action, apply it only to the incoming traffic of an interface.

If you execute the **nest top-most** command multiple times in the same traffic behavior, the most recent configuration takes effect.

Examples

Configure traffic behavior **b1** to add an outer VLAN tag with VLAN ID 123.

```
<Sysname> system-view
[Sysname] traffic behavior b1
[Sysname-behavior-b1] nest top-most vlan 123
```

redirect

Use **redirect** to configure a traffic redirecting action in a traffic behavior.

Use **undo redirect** to restore the default.

Syntax

redirect { **cpu** | **interface** *interface-type interface-number* }

undo redirect { **cpu** | **interface** *interface-type interface-number* }

Default

No traffic redirecting action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

cpu: Redirects traffic to the CPU.

interface *interface-type interface-number*: Redirects traffic to an interface specified by its type and number.

Usage guidelines

If you execute the **redirect** command multiple times in the same traffic behavior, the most recent configuration takes effect.

A traffic redirecting action takes effect only when the QoS policy is applied to the inbound direction.

For traffic redirecting to an access port, make sure the PVID of the interfaces to which the QoS policy is applied is the same as the PVID of the access port. Otherwise, the access port drops redirected packets.

For traffic redirecting to a trunk port, make sure the PVID of the interfaces to which the QoS policy is applied is in the allowed VLAN list of the trunk port. Otherwise, the trunk port drops redirected packets.

If a QoS policy applied to a user profile contains the **redirect interface** action, make sure the redirected-to interface and the incoming interface of packets are in the same VLAN.

Examples

Configure redirecting traffic to GigabitEthernet 1/0/1 in traffic behavior **database**.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] redirect interface gigabitethernet 1/0/1
```

Related commands

classifier behavior

qos policy

traffic behavior

remark dot1p

Use **remark dot1p** to configure an 802.1p priority marking action in a traffic behavior.

Use **undo remark dot1p** to restore the default.

Syntax

remark [**green** | **red** | **yellow**] **dot1p** *dot1p-value*

undo remark [**green** | **red** | **yellow**] **dot1p**

Default

No 802.1p priority marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

green: Specifies green packets.

red: Specifies red packets.

yellow: Specifies yellow packets.

dot1p-value: Specifies the 802.1p priority to be marked for packets, in the range of 0 to 7.

Usage guidelines

If you execute the **remark dot1p** command multiple times for the same color, the most recent configuration takes effect.

Examples

Configure traffic behavior **database** to mark matching traffic with 802.1p 2.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark dot1p 2
```

remark dscp

Use **remark dscp** to configure a DSCP marking action in a traffic behavior.

Use **undo remark dscp** to restore the default.

Syntax

remark [**green** | **red** | **yellow**] **dscp** *dscp-value*

undo remark [**green** | **red** | **yellow**] **dscp**

Default

No DSCP marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

green: Specifies green packets.

red: Specifies red packets.

yellow: Specifies yellow packets.

dscp-value: Specifies a DSCP value, which can be a number from 0 to 63 or a keyword in Table 4.

Table 4 DSCP keywords and values

Keyword	DSCP value (binary)	DSCP value (decimal)
af11	001010	10
af12	001100	12
af13	001110	14
af21	010010	18
af22	010100	20
af23	010110	22
af31	011010	26
af32	011100	28

Keyword	DSCP value (binary)	DSCP value (decimal)
af33	011110	30
af41	100010	34
af42	100100	36
af43	100110	38
cs1	001000	8
cs2	010000	16
cs3	011000	24
cs4	100000	32
cs5	101000	40
cs6	110000	48
cs7	111000	56
default	000000	0
ef	101110	46

Examples

Configure traffic behavior **database** to mark matching traffic with DSCP 6.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark dscp 6
```

remark local-precedence

Use **remark local-precedence** to configure a local precedence marking action in a traffic behavior.

Use **undo remark local-precedence** to restore the default.

Syntax

remark local-precedence *local-precedence-value*

undo remark local-precedence

Default

No local precedence marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

local-precedence-value: Specifies the local precedence to be marked for packets, in the range of 0 to 7.

Usage guidelines

A local precedence marking action takes effect only when the QoS policy is applied to the inbound direction.

Examples

Configure traffic behavior **database** to mark matching traffic with local precedence 2.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark local-precedence 2
```

remark service-vlan-id

Use **remark service-vlan-id** to configure an SVLAN marking action in a traffic behavior.

Use **undo remark service-vlan-id** to restore the default.

Syntax

remark service-vlan-id *vlan-id*

undo remark service-vlan-id

Default

No SVLAN marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies an SVLAN ID in the range of 1 to 4094.

Usage guidelines

An SVLAN marking action can be applied only to an interface.

Examples

Configure traffic behavior **b1** to mark matching packets with SVLAN 222.

```
<Sysname> system-view
[Sysname] traffic behavior b1
[Sysname-behavior-b1] remark service-vlan-id 222
```

traffic behavior

Use **traffic behavior** to create a traffic behavior and enter its view, or enter the view of an existing traffic behavior.

Use **undo traffic behavior** to delete a traffic behavior.

Syntax

traffic behavior *behavior-name*

undo traffic behavior *behavior-name*

Default

No traffic behaviors exist.

Views

System view

Predefined user roles

network-admin

Parameters

behavior-name: Specifies a name for the traffic behavior, a case-sensitive string of 1 to 31 characters.

Examples

Create a traffic behavior named **behavior1**.

```
<Sysname> system-view
[Sysname] traffic behavior behavior1
[Sysname-behavior-behavior1]
```

Related commands

display traffic behavior

QoS policy commands

classifier behavior

Use **classifier behavior** to associate a traffic behavior with a traffic class in a QoS policy.

Use **undo classifier** to delete a class-behavior association from a QoS policy.

Syntax

classifier *classifier-name* **behavior** *behavior-name* [**insert-before** *before-classifier-name*]

undo classifier *classifier-name*

Default

No traffic behavior is associated with a traffic class.

Views

QoS policy view

Predefined user roles

network-admin

Parameters

classifier-name: Specifies a traffic class by its name, a case-sensitive string of 1 to 31 characters.

behavior-name: Specifies a traffic behavior by its name, a case-sensitive string of 1 to 31 characters.

insert-before *before-classifier-name*: Inserts the new traffic class before an existing traffic class in the QoS policy. The *before-classifier-name* argument specifies an existing traffic class by its name, a case-sensitive string of 1 to 31 characters. If you do not specify the **insert-before** *before-classifier-name* option, the new traffic class is placed at the end of the QoS policy.

Usage guidelines

A traffic class can be associated only with one traffic behavior in a QoS policy.

If the specified traffic class or traffic behavior does not exist, the system defines a null traffic class or traffic behavior.

Examples

Associate traffic class **database** with traffic behavior **test** in QoS policy **user1**.

```
<Sysname> system-view
[Sysname] qos policy user1
[Sysname-qospolicy-user1] classifier database behavior test
```

Associate traffic class **database** with traffic behavior **test** in QoS policy **user1**, and insert traffic class **database** before an existing traffic class named **class-a**.

```
<Sysname> system-view
[Sysname] qos policy user1
[Sysname-qospolicy-user1] classifier database behavior test insert-before class-a
```

Related commands

qos policy

display qos policy

Use **display qos policy** to display QoS policies.

Syntax

display qos policy user-defined [*policy-name* [**classifier** *classifier-name*]] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

user-defined: Specifies user-defined QoS policies.

policy-name: Specifies a QoS policy by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a QoS policy, this command displays all user-defined QoS policies.

classifier *classifier-name*: Specifies a traffic class by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a traffic class, this command displays all traffic classes.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the QoS policies for the master device.

Examples

Display all user-defined QoS policies.

```
<Sysname> display qos policy user-defined

  User-defined QoS policy information:

  Policy: 1 (ID 100)
   Classifier: 1 (ID 100)
     Behavior: 1
      Marking:
```

```
      Remark dscp 3
    Committed Access Rate:
      CIR 112 (kbps), CBS 51200 (Bytes), EBS 512 (Bytes)
      Green action  : pass
      Yellow action : pass
      Red action    : discard
  Classifier: 2 (ID 101)
    Behavior: 2
     Accounting enable: Packet
     Filter enable: Permit
     Marking:
      Remark dot1p 4
  Classifier: 3 (ID 102)
    Behavior: 3
     -none-
```

Table 5 Command output

Field	Description
User-defined QoS policy information	Information about a user-defined QoS policy.
System-defined QoS policy information	Information about a system-defined QoS policy.

For the description of other fields, see Table 1 and Table 3.

display qos policy global

Use **display qos policy global** to display QoS policies applied globally.

Syntax

display qos policy global [**slot** *slot-number*] [**inbound** | **outbound**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

inbound: Specifies the QoS policy applied in the inbound direction.

outbound: Specifies the QoS policy applied in the outbound direction.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays global QoS policies for the master device.

Usage guidelines

If you do not specify a direction, this command displays both inbound and outbound global QoS policies.

Examples

Display QoS policies applied globally.

```
<Sysname> display qos policy global
  Direction: Inbound
  Policy: 1
   Classifier: 1
     Operator: AND
     Rule(s) :
      If-match acl 2000
     Behavior: 1
      Marking:
        Remark dscp 3
      Committed Access Rate:
        CIR 112 (kbps), CBS 51200 (Bytes), EBS 512 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets) 0 (Bytes)
        Yellow packets: 0 (Packets) 0 (Bytes)
        Red packets   : 0 (Packets) 0 (Bytes)
   Classifier: 2
     Operator: AND
     Rule(s) :
      If-match protocol ipv6
     Behavior: 2
      Accounting enable:
        0 (Packets)
      Filter enable: Permit
      Marking:
        Remark dscp 3
   Classifier: 3
     Operator: AND
     Rule(s) :
      -none-
     Behavior: 3
      -none-
```

Table 6 Command output

Field	Description
Direction	Direction in which the QoS policy is applied.
Green packets	Statistics about green packets.
Yellow packets	Statistics about yellow packets.
Red packets	Statistics about red packets.

For the description of other fields, see Table 1 and Table 3.

display qos policy interface

Use **display qos policy interface** to display the QoS policies applied to interfaces.

Syntax

display qos policy interface [*interface-type interface-number*] [**inbound** | **outbound**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number.

inbound: Specifies the QoS policy applied to incoming traffic.

outbound: Specifies the QoS policy applied to outgoing traffic.

Usage guidelines

If you do not specify a direction, this command displays the QoS policy applied to incoming traffic and the QoS policy applied to outgoing traffic.

Examples

Display the QoS policy applied to the incoming traffic of GigabitEthernet 1/0/1.

```
<Sysname> display qos policy interface gigabitethernet 1/0/1 inbound
Interface: GigabitEthernet1/0/1
  Direction: Inbound
  Policy: 1
   Classifier: 1
     Matched : 0 (Packets) 0 (Bytes)
     5-minute statistics:
      Forwarded: 0/0 (pps/bps)
      Dropped  : 0/0 (pps/bps)
     Operator: AND
     Rule(s) :
      If-match acl 2000
     Behavior: 1
      Marking:
        Remark dscp 3
      Committed Access Rate:
        CIR 112 (kbps), CBS 51200 (Bytes), EBS 512 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets) 0 (Bytes)
        Yellow packets: 0 (Packets) 0 (Bytes)
        Red packets   : 0 (Packets) 0 (Bytes)
   Classifier: 2
```

```
    Matched : 0 (Packets) 0 (Bytes)
    5-minute statistics:
     Forwarded: 0/0 (pps/bps)
     Dropped  : 0/0 (pps/bps)
    Operator: AND
    Rule(s) :
     If-match protocol ipv6
    Behavior: 2
     Accounting enable:
       0 (Packets)
     Filter enable: Permit
     Marking:
       Remark dscp 3
  Classifier: 3
    Matched : 0 (Packets) 0 (Bytes)
    5-minute statistics:
     Forwarded: 0/0 (pps/bps)
     Dropped  : 0/0 (pps/bps)
    Operator: AND
    Rule(s) :
     -none-
    Behavior: 3
     -none-
```

Display the QoS policies applied to all interfaces.

```
<Sysname> display qos policy interface
Interface: GigabitEthernet1/0/1
  Direction: Inbound
  Policy: a
   Classifier: a
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: a
      Mirroring:
        Mirror to the interface: GigabitEthernet1/0/2
      Committed Access Rate:
        CIR 112 (kbps), CBS 51200 (Bytes), EBS 0 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets)
        Red packets   : 0 (Packets)

Interface: GigabitEthernet1/0/3
  Direction: Inbound
  Policy: b
   Classifier: b
     Operator: AND
```

```
    Rule(s) :
     If-match any
    Behavior: b
     Committed Access Rate:
       CIR 112 (kbps), CBS 51200 (Bytes), EBS 0 (Bytes)
       Green action  : pass
       Yellow action : pass
       Red action    : discard
       Green packets : 0(Packets)
       Red packets   : 0 (Packets)

Interface: GigabitEthernet1/0/4
  Direction: Inbound
  Policy: a
   Classifier: a
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: a
      Mirroring:
        Mirror to the interface: GigabitEthernet1/0/5
      Committed Access Rate:
        CIR 112 (kbps), CBS 51200 (Bytes), EBS 0 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets)
        Red packets   : 0 (Packets)
```

Table 7 Command output

Field	Description
Direction	Direction in which the QoS policy is applied.
Matched	Number of matching packets.
Forwarded	Average rate of successfully forwarded matching packets in a statistics collection period.
Dropped	Average rate of dropped matching packets in a statistics collection period.
Green packets	Traffic statistics for green packets.
Yellow packets	Traffic statistics for yellow packets.
Red packets	Traffic statistics for red packets.

For the description of other fields, see Table 1 and Table 3.

display qos policy user-profile

Use **`display qos policy user-profile`** to display QoS policies applied to user profiles.

Syntax

display qos policy user-profile [**name** *profile-name*] [**user-id** *user-id*] [**slot** *slot-number*] [**inbound** | **outbound**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *profile-name*: Specifies a user profile by its name, a case-sensitive string of 1 to 31 characters. Valid characters include English letters, digits, and underscores (_). The name must start with an English letter and must be unique. If you do not specify a user profile, this command displays QoS policies applied to all user profiles.

user-id *user-id*: Specifies an online user by a system-assigned, hexadecimal ID in the range of 0 to fffffffe. If you do not specify an online user, this command displays QoS policies applied to user profiles for all online users.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays QoS policies applied to user profiles for all member devices.

inbound: Specifies QoS policies applied to incoming traffic.

outbound: Specifies QoS policies applied to outgoing traffic.

Usage guidelines

If you do not specify a direction, this command displays QoS policies applied in the inbound direction and QoS policies applied in the outbound direction.

Examples

Display the QoS policy applied to user profile **abc** for a global user.

```
<Sysname> display qos policy user-profile name abc user-id 30000000 inbound
User-Profile: abc
  User ID: 0x30000000(global)
    Direction: Inbound
    Policy: p1
     Classifier: default-class
       Matched : 0 (Packets) 0 (Bytes)
       Operator: AND
       Rule(s) :
        If-match any
       Behavior: be
         -none-
```

Display the QoS policy applied to user profile **abc** for a local user.

```
<Sysname> display qos policy user-profile name abc user-id 30000001 inbound
User-Profile: abc
  slot 2:
    User ID: 0x30000001(local)
      Direction: Inbound
      Policy: p1
       Classifier: default-class
```

```
Matched : 0 (Packets) 0 (Bytes)
Operator: AND
Rule(s) :
 If-match any
Behavior: be
 -none-
```

Table 8 Command output

Field	Description
global	Indicates a global user, who comes online from a global interface such as an aggregate interface.
local	Indicates a local user, who comes online from a physical interface.
Matched	Number of packets that meet match criteria.
Direction	Direction in which the QoS policy is applied.
Green packets	Statistics about green packets.
Yellow packets	Statistics about yellow packets.
Red packets	Statistics about red packets.

For the description of other fields, see Table 1 and Table 3.

display qos vlan-policy

Use **display qos vlan-policy** to display QoS policies applied to VLANs.

Syntax

display qos vlan-policy { **name** *policy-name* | **vlan** [*vlan-id*] } [**slot** *slot-number*] [**inbound** | **outbound**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *policy-name*: Specifies a QoS policy by its name, a case-sensitive string of 1 to 31 characters.

vlan *vlan-id*: Specifies a VLAN by its ID in the range of 1 to 4094.

inbound: Displays QoS policies applied to incoming traffic.

outbound: Displays QoS policies applied to outgoing traffic.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays QoS policies applied to VLANs for the master device.

Usage guidelines

If you do not specify a direction, this command displays QoS policies applied to VLANs in both the inbound and outbound directions.

Examples

Display QoS policies applied to VLAN 2.

```
<Sysname> display qos vlan-policy vlan 2
Vlan 2
  Direction: Inbound
  Policy: 1
   Classifier: 1
     Operator: AND
     Rule(s) :
      If-match acl 2000
     Behavior: 1
      Marking:
        Remark dscp 3
      Committed Access Rate:
        CIR 112 (kbps), CBS 5120 (Bytes), EBS 512 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0(Packets) 0(Bytes)
        Yellow packets: 0(Packets) 0(Bytes)
        Red packets   : 0(Packets) 0(Bytes)
   Classifier: 2
     Operator: AND
     Rule(s) :
      If-match protocol ipv6
     Behavior: 2
      Accounting enable:
        0 (Packets)
      Filter enable: Permit
      Marking:
        Remark dscp 3
   Classifier: 3
     Operator: AND
     Rule(s) :
      -none-
     Behavior: 3
      -none-
```

Table 9 Command output

Field	Description
Direction	Direction in which the QoS policy is applied.
Green packets	Statistics about green packets.
Yellow packets	Statistics about yellow packets.
Red packets	Statistics about red packets.

For the description of other fields, see Table 1 and Table 3.

qos apply policy (interface view)

Use **qos apply policy** to apply a QoS policy to an interface.

Use **undo qos apply policy** to remove an applied QoS policy.

Syntax

qos apply policy *policy-name* { **inbound** | **outbound** }

undo qos apply policy *policy-name* { **inbound** | **outbound** }

Default

No QoS policy is applied.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a QoS policy by its name, a case-sensitive string of 1 to 31 characters.

inbound: Applies the QoS policy to incoming traffic.

outbound: Applies the QoS policy to outgoing traffic.

Examples

Apply QoS policy **TEST1** to the outgoing traffic of GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos apply policy TEST1 outbound
```

qos apply policy (user profile view)

Use **qos apply policy** to apply a QoS policy to a user profile.

Use **undo qos apply policy** to remove a QoS policy applied to a user profile.

Syntax

qos apply policy *policy-name* { **inbound** | **outbound** }

undo qos apply policy *policy-name* { **inbound** | **outbound** }

Default

No QoS policy is applied to a user profile.

Views

User profile view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a QoS policy by its name, a case-sensitive string of 1 to 31 characters.

inbound: Applies the QoS policy to the incoming traffic of the device (traffic sent by online users).

outbound: Applies the QoS policy to the outgoing traffic of the device (traffic received by online users).

Usage guidelines

Deleting a user profile also removes the QoS policies applied to the user profile.

For a user profile to be active, the QoS policy applied in user profile view cannot be empty. A user profile supports only the **car** and **accounting** actions in a QoS policy.

Examples

Apply QoS policy **test** to incoming traffic of user profile **user**.

```
<Sysname> system-view
[Sysname] user-profile user
[Sysname-user-profile-user] qos apply policy test outbound
```

qos apply policy global

Use **qos apply policy global** to apply a QoS policy globally.

Use **undo qos apply policy global** to remove a globally applied QoS policy.

Syntax

qos apply policy *policy-name* **global** { **inbound** | **outbound** }

undo qos apply policy *policy-name* **global** { **inbound** | **outbound** }

Default

No QoS policy is applied globally.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a QoS policy by its name, a case-sensitive string of 1 to 31 characters.

inbound: Applies the QoS policy to the incoming packets on all interfaces.

outbound: Applies the QoS policy to the outgoing packets on all interfaces.

Usage guidelines

A global QoS policy takes effect on all incoming or outgoing traffic depending on the direction in which the QoS policy is applied.

Examples

Globally apply QoS policy **user1** to the incoming traffic.

```
<Sysname> system-view
[Sysname] qos apply policy user1 global inbound
```

qos policy

Use **qos policy** to create a QoS policy and enter its view, or enter the view of an existing QoS policy.

Use **undo qos policy** to delete a QoS policy.

Syntax

qos policy *policy-name*

undo qos policy *policy-name*

Default

No QoS policies exist.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a name for the QoS policy, a case-sensitive string of 1 to 31 characters.

Usage guidelines

To delete a QoS policy that has been applied to an object, you must first remove the QoS policy from the object.

Examples

Create a QoS policy named **user1**.

```
<Sysname> system-view
[Sysname] qos policy user1
[Sysname-qospolicy-user1]
```

Related commands

classifier behavior

qos apply policy

qos apply policy global

qos vlan-policy

qos vlan-policy

Use **qos vlan-policy** to apply a QoS policy to the specified VLANs.

Use **undo qos vlan-policy** to remove a QoS policy from the specified VLANs.

Syntax

qos vlan-policy *policy-name* **vlan** *vlan-id-list* { **inbound** | **outbound** }

undo qos vlan-policy *policy-name* **vlan** *vlan-id-list* { **inbound** | **outbound** }

Default

No QoS policy is applied to a VLAN.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a QoS policy by its name, a case-sensitive string of 1 to 31 characters.

vlan *vlan-id-list*: Specifies a space-separated list of up to eight VLAN IDs or a VLAN ID range in the form of *vlan-id1* **to** *vlan-id2*. The value for *vlan-id2* must be greater than or equal to the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

inbound: Applies the QoS policy to incoming packets.

outbound: Applies the QoS policy to outgoing packets.

Examples

Apply QoS policy **test** to the incoming traffic of VLAN 200, VLAN 300, VLAN 400, and VLAN 500.

```
<Sysname> system-view
[Sysname] qos vlan-policy test vlan 200 300 400 500 inbound
```

reset qos policy global

Use **reset qos policy global** to clear statistics for QoS policies applied globally.

Syntax

reset qos policy global [**inbound** | **outbound**]

Views

User view

Predefined user roles

network-admin

Parameters

inbound: Specifies the QoS policy applied to the inbound direction globally.

outbound: Specifies the QoS policy applied to the outbound direction globally.

Usage guidelines

If you do not specify a direction, this command clears statistics for the global QoS policies in both directions.

Examples

Clear statistics for the QoS policy applied to the inbound direction globally.

```
<Sysname> reset qos policy global inbound
```

reset qos vlan-policy

Use **reset qos vlan-policy** to clear the statistics for QoS policies applied to VLANs.

Syntax

reset qos vlan-policy [**vlan** *vlan-id*] [**inbound** | **outbound**]

Views

User view

Predefined user roles

network-admin

Parameters

vlan *vlan-id*: Specifies a VLAN ID in the range of 1 to 4094.

inbound: Specifies the QoS policy applied to incoming traffic.

outbound: Specifies the QoS policy applied to outgoing traffic.

Usage guidelines

If you do not specify a direction, this command clears the statistics of the QoS policies in both directions of the VLAN.

Examples

Clear the statistics of QoS policies applied to VLAN 2.

```
<Sysname> reset qos vlan-policy vlan 2
```

Priority mapping commands

Priority map commands

display qos map-table

Use **display qos map-table** to display the configuration of priority maps.

Syntax

display qos map-table [**dot1p-lp** | **dscp-dot1p** | **dscp-dscp**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

The device provides the following types of priority map.

Table 10 Priority maps

Priority mapping	Description
dot1p-lp	802.1p-local priority map.
dscp-dot1p	DSCP-802.1p priority map.
dscp-dscp	DSCP-DSCP priority map.

Usage guidelines

If you do not specify a priority map, this command displays the configuration of all priority maps.

Examples

Display the configuration of the 802.1p-local priority map.

```
<Sysname> display qos map-table dot1p-lp
MAP-TABLE NAME: dot1p-lp   TYPE: pre-define
IMPORT  :  EXPORT
   0    :    2
   1    :    0
   2    :    1
   3    :    3
   4    :    4
   5    :    5
   6    :    6
   7    :    7
```

Table 11 Command output

Field	Description
MAP-TABLE NAME	Name of the priority map.
TYPE	Type of the priority map.
IMPORT	Input values of the priority map.
EXPORT	Output values of the priority map.

import

Use **import** to configure mappings for a priority map.

Use **undo import** to restore the specified or all mappings to the default for a priority map.

Syntax

import *import-value-list* **export** *export-value*

undo import { *import-value-list* | **all** }

Default

The default priority maps are used. For more information, see *ACL and QoS Configuration Guide*.

Views

Priority map view

Predefined user roles

network-admin

Parameters

import-value-list: Specifies a list of input values.

export-value: Specifies the output value.

all: Restores all mappings in the priority map to the default.

Examples

Configure the 802.1p-local priority map to map 802.1p priority values 4 and 5 to local priority 1.

```
<Sysname> system-view
[Sysname] qos map-table dot1p-lp
[Sysname-maptbl-dot1p-lp] import 4 5 export 1
```

Related commands

display qos map-table

qos map-table

Use **qos map-table** to enter the specified priority map view.

Syntax

qos map-table { **dot1p-lp** | **dscp-dot1p** | **dscp-dscp** }

Views

System view

Predefined user roles

network-admin

Parameters

For the description of the keywords, see Table 10.

Examples

Enter 802.1p-local priority map view.

```
<Sysname> system-view
[Sysname] qos map-table dot1p-lp
[Sysname-maptbl-dot1p-lp]
```

Related commands

display qos map-table

import

Priority trust mode commands

display qos trust interface

Use **display qos trust interface** to display the priority trust mode and port priorities of an interface.

Syntax

display qos trust interface [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays the priority trust mode and port priorities of all interfaces.

Examples

Display the priority trust mode and port priority of GigabitEthernet 1/0/1.

```
<Sysname> display qos trust interface gigabitethernet 1/0/1
Interface: GigabitEthernet1/0/1
 Port priority information
  Port priority: 0
  Port dscp priority: -
  Port priority trust type: none
```

Table 12 Command output

Field	Description
Interface	Interface type and interface number.

Field	Description
Port priority	Port priority set for the interface.
Port dscp priority	DSCP value rewritten for packets. If you have not rewritten the DSCP value of packets, this field displays a hyphen (-).
Port priority trust type	Priority trust mode on the interface: • **dot1p**—Uses the 802.1p priority of received packets for mapping. • **dscp**—Uses the DSCP precedence of received IP packets for mapping. • **none**—Trusts no packet priority.

qos trust

Use **qos trust** to configure the priority trust mode for an interface.

Use **undo qos trust** to restore the default.

Syntax

qos trust { **dot1p** | **dscp** }

undo qos trust

Default

An interface does not trust any packet priority and uses the port priority as the 802.1p priority for mapping.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

dot1p: Uses the 802.1p priority in incoming packets for priority mapping.

dscp: Uses the DSCP value in incoming packets for priority mapping.

Examples

Set the priority trust mode to 802.1p priority on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos trust dot1p
```

Related commands

display qos trust interface

Port priority commands

qos priority

Use **qos priority** to change the port priority of an interface.

Use **undo qos priority** to restore the default.

Syntax

qos priority [**dscp**] *priority-value*

undo qos priority [**dscp**]

Default

The port priority is 0.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

priority-value: Specifies a priority value. If the **dscp** keyword is not specified, this argument specifies the port priority in the range of 0 to 7. If the **dscp** keyword is specified, this argument specifies the DSCP value to be set for packets, in the range of 0 to 63.

Examples

Set the port priority of GigabitEthernet 1/0/1 to 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos priority 2
```

Related commands

display qos trust interface

GTS and rate limit commands

GTS commands

display qos gts interface

Use **display qos gts interface** to display the GTS configuration for interfaces.

Syntax

display qos gts interface [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays the GTS configuration for all interfaces.

Examples

Display the GTS configuration for all interfaces.

```
<Sysname> display qos gts interface
Interface: GigabitEthernet1/0/1
 Rule: If-match queue 1
  CIR 512 (kbps), CBS 51200 (Bytes)
```

Table 13 Command output

Field	Description
Interface	Interface name, including the interface type and interface number.
Rule	Match criteria.
CIR	CIR in kbps.
CBS	CBS in bytes.

qos gts

Use **qos gts** to set GTS parameters on an interface.

Use **undo qos gts** to delete the GTS configuration on an interface.

Syntax

qos gts queue *queue-id* **cir** *committed-information-rate* [**cbs** *committed-burst-size*]

undo qos gts queue *queue-id*

Default

No GTS parameters are configured.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

queue *queue-id*: Shapes the packets in a queue specified by its ID. The value range for *queue-id* is 0 to 7.

cir *committed-information-rate*: Specifies the CIR in kbps. The value range for *committed-information-rate* is 8 to 102400 for 100-Mbps interfaces, 8 to 1048576 for GE interfaces, and 8 to 10485760 for 10-GE interfaces. The specified value must be an integral multiple of 8.

cbs *committed-burst-size*: Specifies the CBS in bytes. The value range for *committed-burst-size* is 512 to 16777216, in increments of 512. The default value for this argument is the product of 62.5 and the CIR and must be a multiple of 512. When the product is not a multiple of 512, it is rounded up to the nearest integral multiple of 512 that is greater than the product. A default value greater than 16777216 is converted to 16777216.

Examples

Shape the packets of queue 1 on GigabitEthernet 1/0/1. The GTS parameters are as follows:

- The CIR is 6400 kbps.
- The CBS is 51200 bytes.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos gts queue 1 cir 6400 cbs 51200
```

Rate limit commands

display qos lr interface

Use **display qos lr interface** to display the rate limit configuration for interfaces.

Syntax

display qos lr interface [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays the rate limit configuration for all interfaces.

Examples

Display the rate limit configuration for all interfaces.

```
<Sysname> display qos lr interface
Interface: GigabitEthernet1/0/1
 Direction: Outbound
  CIR 2000 (kbps), CBS 20480 (Bytes)
```

Table 14 Command output

Field	Description
Interface	Interface name, including the interface type and interface number.
Direction	Direction in which the rate limit configuration is applied.
CIR	CIR in kbps.
CBS	CBS in bytes.

qos lr

Use **qos lr** to configure rate limiting on an interface.

Use **undo qos lr** to delete the rate limit configuration on an interface.

Syntax

qos lr { **inbound** | **outbound** } **cir** *committed-information-rate* [**cbs** *committed-burst-size*]

undo qos lr { **inbound** | **outbound** }

Default

No rate limit is configured.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

inbound: Limits the rate of incoming packets.

outbound: Limits the rate of outgoing packets.

cir *committed-information-rate*: Specifies the CIR in kbps. The value range for *committed-information-rate* is 8 to 102400 for 100-Mbps interfaces, 8 to 1048576 for GE interfaces, and 8 to 10485760 for 10-GE interfaces. The specified value must be a multiple of 8.

cbs *committed-burst-size*: Specifies the CBS in bytes. The value range for *committed-burst-size* is 512 to 134217728, in increments of 512. The default value for this argument is the product of 62.5 and the CIR and must be a multiple of 512. When the product is not a multiple of 512, it is rounded up to the nearest integral multiple of 512 that is greater than the product. A default value greater than 134217728 is converted to 134217728.

Examples

Limit the rate of outgoing packets on GigabitEthernet 1/0/1, with CIR 256 kbps and CBS 51200 bytes.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos lr outbound cir 256 cbs 51200
```

Congestion management commands

Common commands

display qos queue interface

Use **display qos queue interface** to display the queuing information for interfaces.

Syntax

display qos queue interface [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays the queuing information for all interfaces.

Examples

Display the queuing information for all interfaces.

```
<Sysname> display qos queue interface
Interface: GigabitEthernet1/0/1
Output queue: Weighted Round Robin queuing
 Queue ID     Queue name     Group     Byte count
 -------------------------------------------------
 0            be             1         1
 1            af1            1         2
 2            af2            1         3
 3            af3            1         4
 4            af4            1         5
 5            ef             1         9
 6            cs6            1         13
 7            cs7            1         15
Interface: GigabitEthernet1/0/2
Output queue: Weighted Round Robin queuing
 Queue ID     Queue name     Group     Byte count
 -------------------------------------------------
 0            be             1         1
 1            af1            1         2
 2            af2            1         3
 3            af3            1         4
 4            af4            1         5
 5            ef             1         9
 6            cs6            1         13
```

```
 7             cs7             1          15
...
```

Table 15 Command output

Field	Description
Interface	Interface name, including the interface type and interface number.
Output queue	Type of the current output queue.
Group	Number of the group that holds the queue.
Weight	Packet-count scheduling weight of the queue. N/A is displayed for a queue that uses the SP scheduling algorithm.

SP commands

display qos queue sp interface

Use **display qos queue sp interface** to display the SP queuing configuration of an interface.

Syntax

display qos queue sp interface [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays the SP queuing configuration of all interfaces.

Examples

Display the SP queuing configuration of GigabitEthernet 1/0/1.

```
<Sysname> display qos queue sp interface gigabitethernet 1/0/1
Interface: GigabitEthernet1/0/1
 Output queue: Strict Priority queuing
```

Table 16 Command output

Field	Description
Interface	Interface type and interface number.
Output queue	Type of the current output queue.

qos sp

Use **qos sp** to enable SP queuing on an interface.

Use **undo qos sp** to restore the default.

Syntax

qos sp

undo qos sp

Default

An interface uses packet-count WRR queuing.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Examples

Enable SP queuing on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos sp
```

Related commands

display qos queue sp interface

WRR commands

display qos queue wrr interface

Use **display qos queue wrr interface** to display the WRR queuing configuration of an interface.

Syntax

display qos queue wrr interface [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays the WRR queuing configuration of all interfaces.

Examples

Display the WRR queuing configuration of GigabitEthernet 1/0/1.

```
<Sysname> display qos queue wrr interface gigabitethernet 1/0/1
Interface: GigabitEthernet1/0/1
 Output queue: Weighted Round Robin queuing
 Queue ID        Queue name      Group           Weight
 ------------------------------------------------------
 0               be              1               1
 1               af1             1               1
```

```
2               af2             1               1
3               af3             1               1
4               af4             1               1
5               ef              1               1
6               cs6             1               1
7               cs7             sp              N/A
```

Table 17 Command output

Field	Description
Interface	Interface type and interface number.
Output queue	Type of the current output queue.
Group	ID of the group a queue is assigned to.
Weight	Packet-count queue scheduling weight of a queue. N/A is displayed for a queue that uses the SP scheduling algorithm.

qos wrr

Use **qos wrr** to enable WRR queuing on an interface.

Use **undo qos wrr** to restore the default.

Syntax

qos wrr weight

undo qos wrr weight

Default

An interface uses packet-count WRR queuing.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

weight: Allocates bandwidth to queues in packets.

Usage guidelines

You must use the **qos wrr** command to enable WRR queuing before you can configure WRR queuing parameters for a queue on an interface.

Examples

Enable packet-count WRR queuing on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wrr weight
```

Related commands

display qos queue wrr interface

qos wrr weight

Use **qos wrr weight** to configure the WRR queuing parameters for a queue on an interface.

Use **undo qos wrr** to restore the default.

Syntax

qos wrr *queue-id* **group 1 weight** *schedule-value*

undo qos wrr *queue-id*

Default

All queues on a WRR-enabled interface are in WRR group 1, and queues 0 through 7 have a weight of 1, 2, 3, 4, 5, 9, 13, and 15, respectively.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

queue-id: Specifies a queue by its ID. The value range for this argument is 0 to 7 or keywords in Table 18.

Table 18 The number-keyword map for the *queue-id* argument

Number	Keyword
0	be
1	af1
2	af2
3	af3
4	af4
5	ef
6	cs6
7	cs7

group 1: Specifies WRR group 1. Only WRR group 1 is supported in the current software version.

weight: Allocates bandwidth to queues in packets.

schedule-value: Specifies a scheduling weight. The value range for this argument is 1 to 15.

Usage guidelines

You must use the **qos wrr** command to enable WRR queuing before you can configure WRR queuing parameters for a queue on an interface.

Examples

Enable packet-based WRR queuing on GigabitEthernet 1/0/1, assign queue 0 to WRR group 1, and specify scheduling weight 10 for queue 0.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wrr weight
```

```
[Sysname-GigabitEthernet1/0/1] qos wrr 0 group 1 weight 10
```

Related commands

display qos queue wrr interface

qos wrr

qos wrr group sp

Use **qos wrr group sp** to assign a queue to the SP group.

Use **undo qos wrr group sp** to remove a queue from the SP group.

Syntax

qos wrr *queue-id* **group sp**

undo qos wrr *queue-id*

Default

All queues on a WRR-enabled interface are in WRR group 1.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

queue-id: Specifies a queue by its ID. The value range for this argument is 0 to 7 or keywords in Table 18.

Usage guidelines

This command is available only on a WRR-enabled interface. Queues in the SP group are scheduled with SP. The SP group has higher scheduling priority than the WRR groups.

You must use the **qos wrr** command to enable WRR queuing before you can configure this command on an interface.

A queue in the SP group is not scheduled if the queue has the lowest priority among all queues with traffic load on the interface.

Examples

Enable WRR queuing on GigabitEthernet 1/0/1, and assign queue 0 to the SP group.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wrr weight
[Sysname-GigabitEthernet1/0/1] qos wrr 0 group sp
```

Related commands

display qos queue wrr interface

qos wrr

Queue scheduling profile commands

display qos qmprofile configuration

Use **display qos qmprofile configuration** to display the queue scheduling profile configuration.

Syntax

display qos qmprofile configuration [*profile-name*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

profile-name: Specifies a queue scheduling profile by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a queue scheduling profile, this command displays the configuration of all queue scheduling profiles.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the queue scheduling profile configuration for the master device.

Examples

Display the configuration of queue scheduling profile **myprofile**.

```
<Sysname> display qos qmprofile configuration myprofile
Queue management profile: myprofile (ID 1)
Queue ID  Type  Group   Schedule   Schedule  Min         Max
                        unit       value     bandwidth   bandwidth
------------------------------------------------------------------------
be        SP    N/A     N/A        N/A       N/A         N/A
af1       SP    N/A     N/A        N/A       N/A         N/A
af2       SP    N/A     N/A        N/A       N/A         N/A
af3       SP    N/A     N/A        N/A       N/A         N/A
af4       SP    N/A     N/A        N/A       N/A         N/A
ef        SP    N/A     N/A        N/A       N/A         N/A
cs6       SP    N/A     N/A        N/A       N/A         N/A
cs7       SP    N/A     N/A        N/A       N/A         N/A
```

Table 19 Command output

Field	Description
Queue management profile	Queue scheduling profile name.
Type	Queue scheduling type: • SP. • WRR.
Group	Priority group to which the queue belongs. The value can only be 1. **N/A** indicates this field is ignored.

Field	Description
Schedule unit	Scheduling unit, which can only be **weight**. **N/A** indicates that this field is ignored.
Schedule value	This field indicates the number of packets scheduled each time. **N/A** indicates that this field is ignored.
Min bandwidth	Minimum guaranteed bandwidth for the queue. **N/A** indicates that this field is ignored.
Max bandwidth	This field is not supported in the current software version. Maximum allowed bandwidth for the queue. **N/A** indicates that this field is ignored.

display qos qmprofile interface

Use **display qos qmprofile interface** to display the queue scheduling profile applied to an interface.

Syntax

display qos qmprofile interface [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays the queue scheduling profiles applied to all interfaces.

Examples

Display the queue scheduling profile applied to GigabitEthernet 1/0/1.

```
<Sysname> display qos qmprofile interface gigabitethernet 1/0/1
Interface: GigabitEthernet1/0/1
Direction: Outbound
 Queue management profile: myprofile
```

Table 20 Command output

Field	Description
Direction	Direction in which the queue scheduling profile is applied.
Queue management profile	Name of the queue scheduling profile applied to the interface.

qos apply qmprofile

Use **qos apply qmprofile** to apply a queue scheduling profile to the outbound direction of an interface.

Use **undo qos apply qmprofile** to restore the default.

Syntax

qos apply qmprofile *profile-name*

undo qos apply qmprofile

Default

No queue scheduling profile is applied to an interface.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

profile-name: Specifies a queue scheduling profile by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

You can apply only one queue scheduling profile to an interface.

Examples

Apply queue scheduling profile **myprofile** to the outbound direction of GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos apply qmprofile myprofile
```

Related commands

display qos qmprofile interface

qos qmprofile

Use **qos qmprofile** to create a queue scheduling profile and enter its view, or enter the view of an existing queue scheduling profile.

Use **undo qos qmprofile** to delete a queue scheduling profile.

Syntax

qos qmprofile *profile-name*

undo qos qmprofile *profile-name*

Default

No user-created queue scheduling profiles exist.

Views

System view

Predefined user roles

network-admin

Parameters

profile-name: Specifies a name for the queue scheduling profile, a case-sensitive string of 1 to 31 characters.

Usage guidelines

To delete a queue scheduling profile already applied to an object, first remove it from the object.

Examples

Create a queue scheduling profile named **myprofile** and enter queue scheduling profile view.

```
<Sysname> system-view
[Sysname] qos qmprofile myprofile
[Sysname-qmprofile-myprofile]
```

Related commands

display qos qmprofile interface

queue

queue

Use **queue** to configure queue scheduling parameters.

Use **undo queue** to delete queue scheduling parameter settings.

Syntax

queue *queue-id* { **sp** | **wrr group** *group-id* **weight** *schedule-value* }

undo queue *queue-id*

Default

All queues in a queue scheduling profile are SP queues.

Views

Queue scheduling profile view

Predefined user roles

network-admin

Parameters

queue-id: Specifies a queue by its ID. The value range for this argument is 0 to 7 or keywords in Table 18.

sp: Enables SP for the queue.

wrr: Enables WRR for the queue.

group *group-id*: Specifies a WRR group by its ID. The group ID can only be 1.

weight: Allocates bandwidth to queues in packets.

schedule-value: Specifies the scheduling weight. The value range for this argument is 1 to 15.

Examples

Create a queue scheduling profile named **myprofile**, and configure queue 0 to use SP.

```
<Sysname> system-view
[Sysname] qos qmprofile myprofile
[Sysname-qmprofile-myprofile] queue 0 sp
```

Create a queue scheduling profile named **myprofile**. Configure queue 1 to meet the following requirements:

- The WRR queuing is used.
- The WRR group is group 1.
- The scheduling weight is 10.

```
<Sysname> system-view
```

```
[Sysname] qos qmprofile myprofile
[Sysname-qmprofile-myprofile] queue 1 wrr group 1 weight 10
```

Related commands

display qos qmprofile interface

qos qmprofile

Queue-based accounting commands

display qos queue-statistics interface outbound

Use **display qos queue-statistics interface outbound** to display queue-based outgoing traffic statistics for interfaces.

Syntax

display qos queue-statistics interface [*interface-type interface-number*] **outbound**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays the queue-based outgoing traffic statistics for all interfaces.

Examples

Display queue-based outgoing traffic statistics for GigabitEthernet 1/0/1.

```
<Sysname> display qos queue-statistics interface gigabitethernet 1/0/1 outbound
Interface: GigabitEthernet1/0/1
 Direction: outbound
 Forwarded: 0 packets, 0 bytes
 Dropped: 0 packets, 0 bytes
 Queue 0
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
 Queue 1
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
 Queue 2
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
 Queue 3
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
```

```
 Dropped: 0 packets, 0 bytes
 Current queue length: 0 packets
Queue 4
 Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
 Dropped: 0 packets, 0 bytes
 Current queue length: 0 packets
Queue 5
 Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
 Dropped: 0 packets, 0 bytes
 Current queue length: 0 packets
Queue 6
 Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
 Dropped: 0 packets, 0 bytes
 Current queue length: 0 packets
Queue 7
 Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
 Dropped: 0 packets, 0 bytes
 Current queue length: 0 packets
```

Table 21 Command output

Field	Description
Interface	Interface for which queue-based traffic statistics are displayed.
Direction	Direction of traffic for which statistics are collected.
Forwarded	Counts forwarded traffic both in packets and in bytes.
Dropped	Counts dropped traffic both in packets and in bytes.
Current queue length	Number of packets in the queue.

Related commands

`reset counters interface` (*Interface Command Reference*)

Aggregate CAR commands

car name

Use **car name** to use an aggregate CAR action in a traffic behavior.

Use **undo car** to restore the default.

Syntax

car name *car-name*

undo car

Default

No aggregate CAR action is configured in a traffic behavior.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

car-name: Specifies the name of an aggregate CAR action. This argument must start with a letter, and is a case-sensitive string of 1 to 31 characters.

Examples

Use aggregate CAR action **aggcar-1** in traffic behavior **be1**.

```
<Sysname> system-view
[Sysname] traffic behavior be1
[Sysname-behavior-be1] car name aggcar-1
```

Related commands

display qos car name

display traffic behavior user-defined

display qos car name

Use **display qos car name** to display information about aggregate CAR actions.

Syntax

display qos car name [*car-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

car-name: Specifies an aggregate CAR action by its name. This argument must start with a letter, and is a case-sensitive string of 1 to 31 characters. If you do not specify an aggregate CAR action, this command displays information about all aggregate CAR actions.

Examples

Display information about all aggregate CAR actions.

```
<Sysname> display qos car name
 Name: a
  Mode: aggregative
   CIR 32 (kbps) CBS: 2048 (Bytes) PIR: 888 (kbps) EBS: 0 (Bytes)
   Green action  : pass
   Yellow action : pass
   Red action    : discard
  Slot 0:
   Green packets : 0 (Packets), 0 (Bytes)
   Yellow packets: 0 (Packets), 0 (Bytes)
   Red packets   : 0 (Packets), 0 (Bytes)
  Slot 1:
   Green packets : 0 (Packets), 0 (Bytes)
   Yellow packets: 0 (Packets), 0 (Bytes)
   Red packets   : 0 (Packets), 0 (Bytes)
  Slot 2:
   Apply failed
```

Table 22 Command output

Field	Description
Name	Name of the aggregate CAR action.
Mode	Type of the CAR action, which can be **aggregative**.
CIR CBS PIR EBS	Parameters for the CAR action.
Green action	Action to take on green packets: • **discard**—Drops the packets. • **pass**—Permits the packets to pass through.
Yellow action	Action to take on yellow packets: • **discard**—Drops the packets. • **pass**—Permits the packets to pass through.
Red action	Action to take on red packets: • **discard**—Drops the packets. • **pass**—Permits the packets to pass through.
Green packets	Statistics about green packets.
Yellow packets	Statistics about yellow packets.
Red packets	Statistics about red packets.

qos car

Use **qos car aggregative** to configure an aggregate CAR action.

Use **undo qos car** to delete an aggregate CAR action.

Syntax

qos car *car-name* **aggregative cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**green** *action* | **red** *action* | **yellow** *action*] *

qos car *car-name* **aggregative cir** *committed-information-rate* [**cbs** *committed-burst-size*] **pir** *peak-information-rate* [**ebs** *excess-burst-size*] [**green** *action* | **red** *action* | **yellow** *action*] *

undo qos car *car-name*

Default

No aggregate CAR action is configured.

Views

System view

Predefined user roles

network-admin

Parameters

car-name: Specifies the name of the aggregate CAR action. This argument must start with a letter, and is a case-sensitive string of 1 to 31 characters.

cir *committed-information-rate*: Specifies the CIR in kbps, which is an average traffic rate. The value range for *committed-information-rate* is 8 to 160000000.

cbs *committed-burst-size*: Specifies the CBS in bytes. The value range for *committed-burst-size* is 512 to 256000000, in increments of 512. The default value for this argument is the product of 62.5 and the CIR and must be an integral multiple of 512. When the product is not an integral multiple of 512, it is rounded up to the nearest integral multiple of 512 that is greater than the product. A default value greater than 256000000 is converted to 256000000.

ebs *excess-burst-size*: Specifies the EBS in bytes. The value range for *excess-burst-size* is 0 to 256000000, in increments of 512. If the PIR is configured, the default EBS is the product of 62.5 and the PIR and must be an integral multiple of 512. When the product is not an integral multiple of 512, it is rounded up to the nearest integral multiple of 512. A default value greater than 256000000 is converted to 256000000.

pir *peak-information-rate*: Specifies the PIR in kbps. The value range for *peak-information-rate* is 8 to 160000000.

green *action*: Specifies the action to take on packets that conform to CIR. The default setting is **pass**.

red *action*: Specifies the action to take on the packet that conforms to neither CIR nor PIR. The default setting is **discard**.

yellow *action*: Specifies the action to take on packets that conform to PIR but not to CIR. The default setting is **pass**.

action: Specifies the action to take on packets:

- **discard**: Drops the packet.
- **pass**: Permits the packet to pass through.
- **remark-dot1p-pass** *new-cos*: Sets the 802.1p priority value of the 802.1p packet to *new-cos* and permits the packet to pass through. The *new-cos* argument is in the range of 0 to 7.

- **remark-dscp-pass** *new-dscp*: Remarks the packet with a new DSCP value and permits the packet to pass through. The *new-dscp* argument is in the range of 0 to 63. Alternatively, you can specify the *new-dscp* argument with **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, **default**, or **ef**.

Usage guidelines

To use two rates for aggregate CAR, configure the **qos car** command with the **pir** *peak-information-rate* option. To use one rate for aggregate CAR, configure the **qos car** command without the **pir** *peak-information-rate* option.

An aggregate CAR action takes effect only after it is used in a QoS policy.

Examples

Configure aggregate CAR action **aggcar-1**, where CIR is 25600, CBS is 512000, and red packets are dropped.

```
<Sysname> system-view
[Sysname] qos car aggcar-1 aggregative cir 25600 cbs 512000 red discard
```

Related commands

display qos car name

reset qos car name

Use **reset qos car name** to clear the statistics about aggregate CAR actions.

Syntax

reset qos car name [*car-name*]

Views

User view

Predefined user roles

network-admin

Parameters

car-name: Specifies an aggregate CAR action by its name. This argument must start with a letter, and is a case-sensitive string of 1 to 31 characters. If you do not specify an aggregate CAR action, this command clears statistics for all aggregate CAR actions.

Examples

Clear the statistics about aggregate CAR action **aggcar-1**.

```
<Sysname> reset qos car name aggcar-1
```

Contents

Data buffer commands

Inappropriate data buffer changes can cause system problems. Before manually changing data buffer settings, make sure you understand its impact on your device. As a best practice, use the **burst-mode enable** command if the system requires large buffer spaces. The **burst-mode enable** command and the **buffer apply** command are mutually exclusive. If you have configured the data buffer by using one command, you must execute the **undo** form of the command before using the other command.

buffer apply

Use **buffer apply** to apply manually configured data buffer settings.

Use **undo buffer apply** to restore the default.

Syntax

buffer apply

undo buffer apply

Views

System view

Predefined user roles

network-admin

Usage guidelines

For data buffer settings to take effect, you must execute this command after configuring data buffer settings.

After applying manually configured data buffer settings, you cannot directly modify the applied settings. To modify them, you must cancel the application, reconfigure data buffer settings, and reapply the new settings.

Examples

Apply manually configured data buffer settings.

```
<Sysname> system-view
[Sysname] buffer apply
```

buffer queue guaranteed

Use **buffer queue guaranteed** to set the fixed-area space for a queue.

Use **undo buffer queue guaranteed** to delete the fixed-area space setting of a queue.

Syntax

buffer egress [**slot** *slot-number*] { **cell** | **packet** } **queue** *queue-id* **guaranteed ratio** *ratio*

undo buffer egress [**slot** *slot-number*] { **cell** | **packet** } **queue** *queue-id* **guaranteed**

Default

The cell resource ratio for a queue is 12% of the total cell resources. The packet resource ratio for a queue is 12% of the total packet resources.

Views

System view

Predefined user roles

network-admin

Parameters

egress: Specifies the egress buffer.

slot *slot-number*: Specifies an IRF member device by its member ID (slot number). If you do not specify an IRF member device, this command applies to all IRF member devices.

cell: Specifies cell resources.

packet: Specifies packet resources.

queue-id: Specifies a queue by its ID in the range of 0 to 7.

ratio *ratio*: Specifies the fixed-area space ratio, in percentage. The value range for *ratio* is 1 to 100.

Usage guidelines

By default, all queues have an equal share of the fixed area. You can set the fixed-area ratio for a queue. The other queues equally share the remaining part.

The fixed-area space for a queue cannot be used by other queues. Therefore, it is also called the minimum guaranteed buffer for the queue. The sum of fixed-area space configured for all queues cannot exceed the total fixed-area space. Otherwise, the configuration fails.

Examples

Configure queue 0 to use 20% fixed-area space of cell resources in the egress buffer.

```
<Sysname> system-view
[Sysname] buffer egress cell queue 0 guaranteed ratio 20
```

buffer shared

Use **buffer shared** to set the maximum shared-area ratio for each port or a queue.

Use **undo buffer shared** to delete the maximum shared-area ratio setting of each port or a queue.

Syntax

buffer egress [**slot** *slot-number*] { **cell** | **packet** } [**queue** *queue-id*] **shared ratio** *ratio*

undo buffer egress [**slot** *slot-number*] { **cell** | **packet** } [**queue** *queue-id*] **shared**

Default

The maximum packet resource ratio for a port is 10% of the total packet resources.

The maximum cell resource ratio for a port is 10% of the total cell resources.

Views

System view

Predefined user roles

network-admin

Parameters

egress: Specifies the egress buffer.

slot *slot-number*: Specifies an IRF member device by its member ID (slot number). If you do not specify an IRF member device, this command applies to all IRF member devices.

cell: Specifies cell resources.

packet: Specifies packet resources.

queue-id: Specifies a queue by its ID in the range of 0 to 7. If you do not specify a queue, this command sets the maximum shared-area space for each port.

ratio *ratio*: Specifies the maximum shared-area space ratio, in percentage. The value range for *ratio* is 0 to 100.

Usage guidelines

By default, all ports or queueshave an equal share of the shared area. You can set the shared-area ratio for each port or a queue. The unconfigured queues use the default setting. The shared-area space for each port or queue is finally determined by the chip based on your configuration and the number of packets to be received and sent.

Examples

Configure queue 0 to use up to 10% shared-area space of cell resources in the egress buffer.

```
<Sysname> system-view
[Sysname] buffer egress cell queue 0 shared ratio 10
```

buffer total-shared

Use **buffer total-shared** to set the total shared-area ratio.

Use **undo buffer total-shared** to delete the total shared-area ratio setting.

Syntax

buffer egress [**slot** *slot-number*] { **cell** | **packet** } **total-shared ratio** *ratio*

undo buffer egress [**slot** *slot-number*] { **cell** | **packet** } **total-shared**

Default

The default for this command can be displayed by using the **display buffer** command.

Views

System view

Predefined user roles

network-admin

Parameters

egress: Specifies the egress buffer.

slot *slot-number*: Specifies an IRF member device by its member ID (slot number). If you do not specify an IRF member device, this command applies to all IRF member devices.

cell: Specifies cell resources.

packet: Specifies packet resources.

ratio *ratio*: Specifies the ratio of the shared area, in percentage. The value range for *ratio* is 0 to 100.

Usage guidelines

After you set the shared-area ratio, the remaining buffer space is automatically assigned to the fixed area.

Examples

Configure the shared area to use 50% space of cell resources in the egress buffer.

```
<Sysname> system-view
[Sysname] buffer egress cell total-shared ratio 50
```

burst-mode enable

Use **burst-mode enable** to enable the Burst feature.

Use **undo burst-mode enable** to disable the Burst feature.

Syntax

burst-mode enable

undo burst-mode enable

Default

The Burst feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The Burst feature is especially useful for reducing packet losses under the following circumstances:

- Broadcast or multicast traffic is intensive, resulting in bursts of traffic.
- Traffic enters a device from a high-speed interface and goes out of a low-speed interface.
- Traffic enters a device from multiple same-rate interfaces and goes out of an interface with the same rate.

The default data buffer settings will be changed after the Burst feature is enabled. You can display the data buffer settings by using the **display buffer** command.

Examples

Enable the Burst feature.

```
<Sysname> system-view
[Sysname] burst-mode enable
```

display buffer

Use **display buffer** to display buffer size settings.

Syntax

display buffer [**slot** *slot-number*][**queue** [*queue-id*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID (slot number). If you do not specify an IRF member device, this command displays buffer size settings for all IRF member devices.

queue *queue-id*: Specifies a queue by its number in the range of 0 to 7. If you specify a queue, this command displays the fixed-area ratio and shared-area ratio for the specified queue. If you specify the **queue** keyword without the *queue-id* argument, this command displays the fixed-area ratio and shared-area ratio for each queue. If you do not specify the **queue** keyword, this command displays the total shared-area ratio.

Examples

Display buffer size settings.

```
<Sysname> display buffer
Slot  Type    Eg(Total-shared , Shared)
1     packet  0 , 20
1     cell    0 , 20

          Eg: Size of the sending buffer
Total-shared: Size of the shared buffer for all ports
      Shared: Size of the maximum shared buffer per port
        Unit: Ratio
```

Display the fixed-area ratio and shared-area ratio for the queues.

```
<Sysname> display buffer queue
Slot  Queue        Type    Eg(Guaranteed , Shared)
1     0-7          packet  12 , --
1     0-7          cell    12 , --

          Eg: Size of the sending buffer
  Guaranteed: Size of the minimum guaranteed buffer per queue
      Shared: Size of the maximum shared buffer per queue
        Unit: Ratio
```

Table 1 Command output

Field	Description
Type	Resource type: packet or cell.
Queue	Queue ID in the range of 0 to 7.
Eg	Egress buffer.
(Total-shared , Shared)	Total-shared indicates the total shared-area ratio. Shared indicates the shared-area ratio of a port.

Field	Description
(Guaranteed , Shared)	• **Guaranteed** indicates the fixed-area ratio of a queue. • **Shared** indicates the shared-area ratio of a queue. If the device does not support a resource type, this field displays two hyphens (--).

display buffer usage

Use **display buffer usage** to display buffer usage.

Syntax

display buffer usage [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID (slot number). If you do not specify an IRF member device, this command displays buffer usage for all IRF member devices.

Examples

Display buffer usage.

```
<Sysname> display buffer usage
Egress total-shared cell buffer usage on slot 1 :
Total:    2980 KB
Used:       0 KB
Free:    2980 KB
                              5sec    1min    5min
-------------------------------------------------------------------
Block 1                        0%      0%      0%
GigabitEthernet1/0/1           0%      0%      0%
GigabitEthernet1/0/2           0%      0%      0%
GigabitEthernet1/0/3           0%      0%      0%
GigabitEthernet1/0/4           0%      0%      0%
GigabitEthernet1/0/5           0%      0%      0%
```

Table 2 Command output

Field	Description
Egress total-shared cell buffer usage on slot	Usage of cell resources in the shared area on an IRF member device.
Block	Block where the port resides. The block where the ports on the front panel of the device reside is fixed to Block 1.
Total	Total size of the data buffer.

Field	Description
Used	Size of used data buffer.
Free	Size of free data buffer.
5sec	Percentage of the buffer that the port uses for the last 5 seconds.
1min	Percentage of the buffer that the port uses for the last 1 minute.
5min	Percentage of the buffer that the port uses for the last 5 minutes.

Contents

Time range commands

display time-range

Use **display time-range** to display time range configuration and status.

Syntax

display time-range { *time-range-name* | **all** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

time-range-name: Specifies a time range name, a case-insensitive string of 1 to 32 characters. It must start with an English letter.

all: Displays the configuration and status of all existing time ranges.

Examples

Display the configuration and status of time range **t4**.

```
<Sysname> display time-range t4
Current time is 17:12:34 11/23/2010 Tuesday

Time-range : t4 (Inactive)
 10:00 to 12:00 Mon
 14:00 to 16:00 Wed
 from 00:00 1/1/2011 to 00:00 1/1/2012
 from 00:00 6/1/2011 to 00:00 7/1/2011
```

Table 1 Command output

Field	Description
Current time	Current system time.
Time-range	Configuration and status of the time range, including its name, status (active or inactive), and start time and end time.

time-range

Use **time-range** to create or edit a time range.

Use **undo time-range** to delete a time range or a statement in the time range.

Syntax

time-range *time-range-name* { *start-time* **to** *end-time days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2* }

undo time-range *time-range-name* [*start-time* **to** *end-time days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2*]

Default

No time ranges exist.

Views

System view

Predefined user roles

network-admin

Parameters

time-range-name: Specifies a time range name. The name is a case-insensitive string of 1 to 32 characters. It must start with an English letter. To avoid confusion, it cannot be **all**.

start-time **to** *end-time*: Specifies a periodic statement. Both *start-time* and *end-time* are in hh:mm format (24-hour clock). The value is in the range of 00:00 to 23:59 for the start time, and 00:00 to 24:00 for the end time. The end time must be later than the start time.

days: Specifies the day or days of the week (in words or digits) on which the periodic statement is valid. If you specify multiple values, separate each value with a space, and make sure they do not overlap. These values can take one of the following forms:

- A digit in the range of 0 to 6, for Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday.
- A day of a week in abbreviated words: **Sun**, **Mon**, **Tue**, **Wed**, **Thu**, **Fri**, and **Sat**.
- **working-day** for Monday through Friday.
- **off-day** for Saturday and Sunday.
- **daily** for the whole week.

from *time1 date1*: Specifies the start time and date of an absolute statement. The *time1* argument specifies the time of the day in hh:mm format (24-hour clock). Its value is in the range of 00:00 to 23:59. The *date1* argument specifies a date in MM/DD/YYYY or YYYY/MM/DD format, where MM is the month of the year in the range of 1 to 12, DD is the day of the month with the range varying by MM, and YYYY is the year in the calendar in the range of 1970 to 2100. If you do not specify this option, the start time is 01/01/1970 00:00 AM, the earliest time available in the system.

to *time2 date2*: Specifies the end time and date of the absolute time statement. The *time2* argument has the same format as the *time1* argument, but its value is in the range of 00:00 to 24:00. The *date2* argument has the same format and value range as the *date1* argument. The end time must be later than the start time. If you do not specify this option, the end time is 12/31/2100 24:00 PM, the maximum time available in the system.

Usage guidelines

If an existing time range name is provided, this command adds a statement to the time range.

You can create multiple statements in a time range. Each time statement can take one of the following forms:

- Periodic statement in the *start-time* **to** *end-time days* format. A periodic statement recurs periodically on a day or days of the week.
- Absolute statement in the **from** *time1 date1* **to** *time2 date2* format. An absolute statement does not recur.
- Compound statement in the *start-time* **to** *end-time days* **from** *time1 date1* **to** *time2 date2* format. A compound statement recurs on a day or days of the week only within the specified period. For example, to create a time range that is active from 08:00 to 12:00 on

Monday between January 1, 2015, 00:00 and December 31, 2015, 23:59, use the **time-range test 08:00 to 12:00 Mon from 00:00 01/01/2015 to 23:59 12/31/2015** command.

You can create a maximum of 1024 time ranges, each with a maximum of 32 periodic statements and 12 absolute statements. The active period of a time range is calculated as follows:

1. Combining all periodic statements.
2. Combining all absolute statements.
3. Taking the intersection of the two statement sets as the active period of the time range.

Examples

Create a periodic time range **t1**, setting it to be active between 8:00 to 18:00 during working days.

```
<Sysname> system-view
[Sysname] time-range t1 08:00 to 18:00 working-day
```

Create an absolute time range **t2**, setting it to be active in the whole year of 2011.

```
<Sysname> system-view
[Sysname] time-range t2 from 00:00 1/1/2011 to 24:00 12/31/2011
```

Create a compound time range **t3**, setting it to be active from 08:00 to 12:00 on Saturdays and Sundays of the year 2011.

```
<Sysname> system-view
[Sysname] time-range t3 08:00 to 12:00 off-day from 00:00 1/1/2011 to 24:00 12/31/2011
```

Create a compound time range **t4**, setting it to be active from 10:00 to 12:00 on Mondays and from 14:00 to 16:00 on Wednesdays in January and June of the year 2011.

```
<Sysname> system-view
[Sysname] time-range t4 10:00 to 12:00 1 from 00:00 1/1/2011 to 24:00 1/31/2011
[Sysname] time-range t4 14:00 to 16:00 3 from 00:00 6/1/2011 to 24:00 6/30/2011
```

Related commands

display time-range

Security Command Reference

This command reference is applicable to the following switches and software versions:

H3C S5120V2-LI switch series (Release 6308P01 and later)
H3C S3100V3-SI switch series (Release 6309P01 and later)
H3C S5110V2 switch series (Release 6310 and later)
H3C S5110V2-SI switch series (Release 6310 and later)
H3C S5000V3-EI switch series (Release 6310 and later)
H3C S5000V5-EI switch series (Release 6319P01 and later)
H3C S5000E-X switch series (Release 6310 and later)
H3C S5130S-LI switch series (Release 6310 and later)
H3C MS4320V2 switch series (Release 6308P01 and later)
H3C MS4320 switch series (Release 6308P01 and later)
H3C MS4300V2 switch series (Release 6308P01 and later)
H3C MS4200 switch series (Release 6310 and later)
H3C WS5810-WiNet switch series (Release 6308P01 and later)
H3C WS5820-WiNet switch series (Release 6308P01 and later)
H3C WAS6000 switch series (Release 6308P01 and later)
H3C S5000X-EI switch series (Release 6329 and later)
H3C MS4320V3 switch series (Release 6329 and later)
H3C S5120V3-SI switch series (Release 6329 and later)
H3C S5120V3-LI switch series (Release 6329 and later)

New H3C Technologies Co., Ltd.
http://www.h3c.com

Software version: Release 63xx
Document version: 6W105-20230524

Preface

This command reference describes the security configuration commands. It includes the commands for configuring the following features:

This preface includes the following topics about the documentation:

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Documentation feedback

You can e-mail your comments about product documentation to info@h3c.com.

We appreciate your comments.

Contents

AAA commands

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

General AAA commands

aaa nas-id profile

Use **aaa nas-id profile** to create a NAS-ID profile and enter its view, or enter the view of an existing NAS-ID profile.

Use **undo aaa nas-id profile** to delete a NAS-ID profile.

Syntax

aaa nas-id profile *profile-name*

undo aaa nas-id profile *profile-name*

Default

No NAS-ID profiles exist.

Views

System view

Predefined user roles

network-admin

Parameters

profile-name: Specifies the NAS-ID profile name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

Configure a NAS-ID profile to maintain NAS-ID and VLAN bindings on the device.

During RADIUS authentication, the device uses a NAS-ID to set the NAS-Identifier attribute of RADIUS packets so that the RADIUS server can identify the access location of users.

By default, the device uses the device name as the NAS-ID.

Examples

Create a NAS-ID profile named **aaa** and enter its view.

```
<Sysname> system-view
[Sysname] aaa nas-id profile aaa
[Sysname-nas-id-prof-aaa]
```

Related commands

nas-id bind vlan

port-security nas-id-profile

portal nas-id-profile

aaa session-limit

Use **aaa session-limit** to set the maximum number of concurrent users that can log on to the device through the specified method.

Use **undo aaa session-limit** to restore the default maximum number of concurrent users for the specified login method.

Syntax

In non-FIPS mode:

aaa session-limit { **ftp** | **http** | **https** | **ssh** | **telnet** } *max-sessions*

undo aaa session-limit { **ftp** | **http** | **https** | **ssh** | **telnet** }

In FIPS mode:

aaa session-limit { **https** | **ssh** } *max-sessions*

undo aaa session-limit { **https** | **ssh** }

Default

The maximum number of concurrent users is 32 for each user type.

Views

System view

Predefined user roles

network-admin

Parameters

ftp: FTP users.

http: HTTP users.

https: HTTPS users.

ssh: SSH users.

telnet: Telnet users.

max-sessions: Specifies the maximum number of concurrent login users. The value range is 1 to 32 for FTP, SSH, and Telnet services, and is 1 to 64 for HTTP and HTTPS services.

Usage guidelines

After the maximum number of concurrent login users for a user type exceeds the upper limit, the system denies the subsequent users of this type.

Examples

Set the maximum number of concurrent FTP users to 4.

```
<Sysname> system-view
[Sysname] aaa session-limit ftp 4
```

accounting command

Use **accounting command** to specify the command line accounting method.

Use **undo accounting command** to restore the default.

Syntax

accounting command hwtacacs-scheme *hwtacacs-scheme-name*

undo accounting command

Default

The default accounting methods of the ISP domain are used for command line accounting.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

The command line accounting feature works with the accounting server to record valid commands that have been successfully executed on the device.

- When the command line authorization feature is disabled, the accounting server records all valid commands that have been successfully executed.
- When the command line authorization feature is enabled, the accounting server records only authorized commands that have been successfully executed.

Command line accounting can use only a remote HWTACACS server.

Examples

In ISP domain **test**, perform command line accounting based on HWTACACS scheme **hwtac**.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting command hwtacacs-scheme hwtac
```

Related commands

accounting default

command accounting (*Fundamentals Command Reference*)

hwtacacs scheme

accounting default

Use **accounting default** to specify default accounting methods for an ISP domain.

Use **undo accounting default** to restore the default.

Syntax

In non-FIPS mode:

accounting default { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }

undo accounting default

In FIPS mode:

accounting default { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] | **local** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] }

undo accounting default

Default

The default accounting method of an ISP domain is local.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local accounting.

none: Does not perform accounting.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

The default accounting method is used for all users that support this method and do not have an accounting method configured.

Local accounting is only used for monitoring and controlling the number of local user connections. It does not provide the statistics function that the accounting feature generally provides.

You can specify one primary default accounting method and multiple backup default accounting methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **accounting default radius-scheme** *radius-scheme-name* **local none** command specifies the primary default RADIUS accounting method and two backup methods (local accounting and no accounting). The device performs RADIUS accounting by default and performs local accounting when the RADIUS server is invalid. The device does not perform accounting when both of the previous methods are invalid.

Examples

In ISP domain **test**, use RADIUS scheme **rd** as the primary default accounting method and use local accounting as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting default radius-scheme rd local
```

Related commands

hwtacacs scheme

local-user

radius scheme

accounting lan-access

Use **accounting lan-access** to specify accounting methods for LAN users.

Use **undo accounting lan-access** to restore the default.

Syntax

In non-FIPS mode:

accounting lan-access { **broadcast radius-scheme** *radius-scheme-name1* **radius-scheme** *radius-scheme-name2* [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo accounting lan-access

In FIPS mode:

accounting lan-access { **broadcast radius-scheme** *radius-scheme-name1* **radius-scheme** *radius-scheme-name2* [**local**] | **local** | **radius-scheme** *radius-scheme-name* [**local**] }

undo accounting lan-access

Default

The default accounting methods of the ISP domain are used for LAN users.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

broadcast: Broadcasts accounting requests to servers in RADIUS schemes.

radius-scheme *radius-scheme-name1*: Specifies the primary broadcast RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

radius-scheme *radius-scheme-name2*: Specifies the backup broadcast RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local accounting.

none: Does not perform accounting.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

You can specify one primary accounting method and multiple backup accounting methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **accounting lan-access radius-scheme** *radius-scheme-name* **local none** command specifies a primary RADIUS accounting method and two backup methods (local accounting and no accounting). The device performs RADIUS accounting by default and performs local accounting when the RADIUS server is invalid. The device does not perform accounting when both of the previous methods are invalid.

The following guidelines apply to broadcast accounting:

- The device sends accounting requests to the primary accounting servers in the specified broadcast RADIUS schemes at the real-time accounting interval set in the primary broadcast RADIUS scheme. If the primary server is unavailable in a scheme, the device sends accounting requests to the secondary servers of the scheme in the order the servers are configured.
- The accounting result is determined by the primary broadcast RADIUS scheme. The accounting result from the backup scheme is used as reference only. If the primary scheme does not return any result, the device considers the accounting as a failure.

Examples

In ISP domain **test**, perform local accounting for LAN users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting lan-access local
```

In ISP domain **test**, perform RADIUS accounting for LAN users based on scheme **rd** and use local accounting as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting lan-access radius-scheme rd local
```

In ISP domain **test**, broadcast accounting requests of LAN users to RADIUS servers in schemes **rd1** and **rd2**, and use local accounting as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting lan-access broadcast radius-scheme rd1 radius-scheme rd2
local
```

Related commands

accounting default

local-user

radius scheme

timer realtime-accounting

accounting login

Use **accounting login** to specify accounting methods for login users.

Use **undo accounting login** to restore the default.

Syntax

In non-FIPS mode:

accounting login { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }

undo accounting login

In FIPS mode:

accounting login { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] | **local** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] }

undo accounting login

Default

The default accounting methods of the ISP domain are used for login users.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local accounting.

none: Does not perform accounting.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

Accounting is not supported for FTP, SFTP, and SCP users.

You can specify one primary accounting method and multiple backup accounting methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **accounting login radius-scheme** *radius-scheme-name* **local none** command specifies a primary default RADIUS accounting method and two backup methods (local accounting and no accounting). The device performs RADIUS accounting by default and performs local accounting when the RADIUS server is invalid. The device does not perform accounting when both of the previous methods are invalid.

Examples

In ISP domain **test**, perform local accounting for login users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting login local
```

In ISP domain **test**, perform RADIUS accounting for login users based on scheme **rd** and use local accounting as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting login radius-scheme rd local
```

Related commands

accounting default

hwtacacs scheme

local-user

radius scheme

accounting portal

Use **accounting portal** to specify accounting methods for portal users.

Use **undo accounting portal** to restore the default.

Syntax

In non-FIPS mode:

accounting portal { **broadcast radius-scheme** *radius-scheme-name1* **radius-scheme** *radius-scheme-name2* [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo accounting portal

In FIPS mode:

accounting portal { **broadcast radius-scheme** *radius-scheme-name1* **radius-scheme** *radius-scheme-name2* [**local**] | **local** | **radius-scheme** *radius-scheme-name* [**local**] }

undo accounting portal

Default

The default accounting methods of the ISP domain are used for portal users.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

broadcast: Broadcasts accounting requests to servers in RADIUS schemes.

radius-scheme *radius-scheme-name1*: Specifies the primary broadcast RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

radius-scheme *radius-scheme-name2*: Specifies the backup broadcast RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local accounting.

none: Does not perform accounting.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

You can specify one primary accounting method and multiple backup accounting methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **accounting portal radius-scheme** *radius-scheme-name* **local none** command specifies a primary default RADIUS accounting method and two backup methods (local accounting and no accounting). The device performs RADIUS accounting by default and performs local accounting when the RADIUS server is invalid. The device does not perform accounting when both of the previous methods are invalid.

The following guidelines apply to broadcast accounting:

- The device sends accounting requests to the primary accounting servers in the specified broadcast RADIUS schemes at the real-time accounting interval set in the primary broadcast RADIUS scheme. If the primary server is unavailable in a scheme, the device sends accounting requests to the secondary servers of the scheme in the order the servers are configured.
- The accounting result is determined by the primary broadcast RADIUS scheme. The accounting result from the backup scheme is used as reference only. If the primary scheme does not return any result, the device considers the accounting as a failure.

Examples

In ISP domain **test**, perform local accounting for portal users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting portal local
```

In ISP domain **test**, perform RADIUS accounting for portal users based on scheme **rd** and use local accounting as the backup.

```
<Sysname> system-view
[Sysname] domain test
```

```
[Sysname-isp-test] accounting portal radius-scheme rd local
```

In ISP domain **test**, broadcast accounting requests of portal users to RADIUS servers in schemes **rd1** and **rd2**, and use local accounting as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting portal broadcast radius-scheme rd1 radius-scheme rd2 local
```

Related commands

accounting default

local-user

radius scheme

timer realtime-accounting

accounting quota-out

Use **accounting quota-out** to configure access control for users that have used up their data or time accounting quotas.

Use **undo accounting quota-out** to restore the default.

Syntax

accounting quota-out { **offline** | **online** }

undo accounting quota-out

Default

The device logs off users that have used up their accounting quotas.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

offline: Logs off users that have used up their accounting quotas.

online: Allows users that have used up their accounting quotas to stay online.

Usage guidelines

If the server notifies the device of portal users' remaining accounting quotas, the time that the device logs out portal users that have used up their accounting quotas might be inaccurate.

Examples

In ISP domain **test**, configure the device to allow users that have used up their accounting quotas to stay online.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting quota-out online
```

accounting start-fail

Use **accounting start-fail** to configure access control for users that encounter accounting-start failures.

Use **undo accounting start-fail** to restore the default.

Syntax

accounting start-fail { **offline** | **online** }

undo accounting start-fail

Default

The device allows users that encounter accounting-start failures to stay online.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

offline: Logs off users that encounter accounting-start failures.

online: Allows users that encounter accounting-start failures to stay online.

Examples

In ISP domain **test**, configure the device to allow users that encounter accounting-start failures to stay online.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting start-fail online
```

accounting update-fail

Use **accounting update-fail** to configure access control for users that have failed all their accounting-update attempts.

Use **undo accounting update-fail** to restore the default.

Syntax

accounting update-fail { [**max-times** *max-times*] **offline** | **online** }

undo accounting update-fail

Default

The device allows users that have failed all their accounting-update attempts to stay online.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

max-times *max-times*: Specifies the maximum number of consecutive accounting-update failures allowed by the device for each user. The value range for the *times* argument is 1 to 255, and the default value is 1.

offline: Logs off users that have failed all their accounting-update attempts.

online: Allows users that have failed all their accounting-update attempts to stay online.

Examples

In ISP domain **test**, configure the device to allow users that have failed all their accounting-update attempts to stay online.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting update-fail online
```

authentication default

Use **authentication default** to specify default authentication methods for an ISP domain.

Use **undo authentication default** to restore the default.

Syntax

In non-FIPS mode:

authentication default { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **ldap-scheme** *ldap-scheme-name* [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }

undo authentication default

In FIPS mode:

authentication default { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] | **ldap-scheme** *ldap-scheme-name* [**local**] | **local** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] }

undo authentication default

Default

The default authentication method of an ISP domain is local.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

ldap-scheme *ldap-scheme-name*: Specifies an LDAP scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local authentication.

none: Does not perform authentication.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

The default authentication method is used for all users that support this method and do not have an authentication method configured.

You can specify one primary default authentication method and multiple backup default authentication methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **authentication default radius-scheme** *radius-scheme-name* **local none** command specifies a primary default RADIUS authentication method and two backup methods (local authentication and no authentication). The device performs RADIUS authentication by default and performs local authentication when the RADIUS server is invalid. The device does not perform authentication when both of the previous methods are invalid.

Examples

In ISP domain **test**, use RADIUS scheme **rd** as the primary default authentication method and use local authentication as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication default radius-scheme rd local
```

Related commands

hwtacacs scheme

ldap scheme

local-user

radius scheme

authentication lan-access

Use **authentication lan-access** to specify authentication methods for LAN users.

Use **undo authentication lan-access** to restore the default.

Syntax

In non-FIPS mode:

authentication lan-access { **ldap-scheme** *ldap-scheme-name* [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authentication lan-access

In FIPS mode:

authentication lan-access { **ldap-scheme** *ldap-scheme-name* [**local**] | **local** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authentication lan-access

Default

The default authentication methods of the ISP domain are used for LAN users.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

ldap-scheme *ldap-scheme-name*: Specifies an LDAP scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local authentication.

none: Does not perform authentication.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

You can specify one primary authentication method and multiple backup authentication methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **authentication lan-access radius-scheme** *radius-scheme-name* **local none** command specifies a primary RADIUS authentication method and two backup methods (local authentication and no authentication). The device performs RADIUS authentication by default and performs local authentication when the RADIUS server is invalid. The device does not perform authentication when both of the previous methods are invalid.

Examples

In ISP domain **test**, perform local authentication for LAN users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication lan-access local
```

In ISP domain **test**, perform RADIUS authentication for LAN users based on scheme **rd** and use local authentication as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication lan-access radius-scheme rd local
```

Related commands

authentication default

hwtacacs scheme

ldap scheme

local-user

radius scheme

authentication login

Use **authentication login** to specify authentication methods for login users.

Use **undo authentication login** to restore the default.

Syntax

In non-FIPS mode:

authentication login { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **ldap-scheme** *ldap-scheme-name* [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }

undo authentication login

In FIPS mode:

authentication login { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] | **ldap-scheme** *ldap-scheme-name* [**local**] | **local** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] }

undo authentication login

Default

The default authentication methods of the ISP domain are used for login users.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

ldap-scheme *ldap-scheme-name*: Specifies an LDAP scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local authentication.

none: Does not perform authentication.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

You can specify one primary authentication method and multiple backup authentication methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **authentication login radius-scheme** *radius-scheme-name* **local none** command specifies the default primary RADIUS authentication method and two backup methods (local authentication and no authentication). The device performs RADIUS authentication by default and performs local authentication when the RADIUS server is invalid. The device does not perform authentication when both of the previous methods are invalid.

Examples

In ISP domain **test**, perform local authentication for login users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication login local
```

In ISP domain **test**, perform RADIUS authentication for login users based on scheme **rd** and use local authentication as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication login radius-scheme rd local
```

Related commands

authentication default

hwtacacs scheme

ldap scheme

local-user

radius scheme

authentication portal

Use **authentication portal** to specify authentication methods for portal users.

Use **undo authentication portal** to restore the default.

Syntax

In non-FIPS mode:

authentication portal { **ldap-scheme** *ldap-scheme-name* [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authentication portal

In FIPS mode:

authentication portal { **ldap-scheme** *ldap-scheme-name* [**local**] | **local** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authentication portal

Default

The default authentication methods of the ISP domain are used for portal users.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

ldap-scheme *ldap-scheme-name*: Specifies an LDAP scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local authentication.

none: Does not perform authentication.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

You can specify one primary authentication method and multiple backup authentication methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **authentication portal radius-scheme** *radius-scheme-name* **local none** command specifies the default primary RADIUS authentication method and two backup methods (local authentication and no authentication). The device performs RADIUS authentication by default and performs local authentication when the RADIUS server is invalid. The device does not perform authentication when both of the previous methods are invalid.

Examples

In ISP domain **test**, perform local authentication for portal users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication portal local
```

In ISP domain **test**, perform RADIUS authentication for portal users based on scheme **rd** and use local authentication as the backup.

```
<Sysname> system-view
[Sysname] domain test
```

```
[Sysname-isp-test] authentication portal radius-scheme rd local
```

Related commands

authentication default

ldap scheme

local-user

radius scheme

authentication super

Use **authentication super** to specify a method for user role authentication.

Use **undo authentication super** to restore the default.

Syntax

authentication super { **hwtacacs-scheme** *hwtacacs-scheme-name* | **radius-scheme** *radius-scheme-name* } *

undo authentication super

Default

The default authentication methods of the ISP domain are used for user role authentication.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

To enable a user to obtain another user role without reconnecting to the device, you must configure user role authentication. The device supports local and remote methods for user role authentication. For more information about user role authentication, see RBAC configuration in *Fundamentals Configuration Guide*.

You can specify one authentication method and one backup authentication method to use in case that the previous authentication method is invalid.

Examples

In ISP domain **test**, perform user role authentication based on HWTACACS scheme **tac**.

```
<Sysname> system-view
[Sysname] super authentication-mode scheme
[Sysname] domain test
[Sysname-isp-test] authentication super hwtacacs-scheme tac
```

Related commands

authentication default

hwtacacs scheme

radius scheme

authorization command

Use **authorization command** to specify command authorization methods.

Use **undo authorization command** to restore the default.

Syntax

In non-FIPS mode:

authorization command { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] [**none**] | **local** [**none**] | **none** }

undo authorization command

In FIPS mode:

authorization command { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** }

undo authorization command

Default

The default authorization methods of the ISP domain are used for command authorization.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local authorization.

none: Does not perform authorization. The authorization server does not verify whether the entered commands are permitted by the user role. The commands are executed successfully if the user role has permission to the commands.

Usage guidelines

Command authorization restricts login users to execute only authorized commands by employing an authorization server to verify whether each entered command is permitted.

When local command authorization is configured, the device compares each entered command with the user's configuration on the device. The command is executed only when it is permitted by the user's authorized user roles.

The commands that can be executed are controlled by both the access permission of user roles and command authorization of the authorization server. Access permission only controls whether the authorized user roles have access to the entered commands, but it does not control whether the user roles have obtained authorization to these commands. If a command is permitted by the access permission but denied by command authorization, this command cannot be executed.

You can specify one primary command authorization method and multiple backup command authorization methods.

When the default authorization method is invalid, the device attempts to use the backup authorization methods in sequence. For example, the **authorization command hwtacacs-scheme** *hwtacacs-scheme-name* **local none** command specifies the default

HWTACACS authorization method and two backup methods (local authorization and no authorization). The device performs HWTACACS authorization by default and performs local authorization when the HWTACACS server is invalid. The device does not perform command authorization when both of the previous methods are invalid.

Examples

In ISP domain **test**, configure the device to perform local command authorization.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization command local
```

In ISP domain **test**, perform command authorization based on HWTACACS scheme **hwtac** and use local authorization as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization command hwtacacs-scheme hwtac local
```

Related commands

command authorization (*Fundamentals Command Reference*)

hwtacacs scheme

local-user

authorization default

Use **authorization default** to specify default authorization methods for an ISP domain.

Use **undo authorization default** to restore the default.

Syntax

In non-FIPS mode:

authorization default { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }

undo authorization default

In FIPS mode:

authorization default { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] | **local** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] }

undo authorization default

Default

The default authorization method of an ISP domain is local.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local authorization.

none: Does not perform authorization. The following default authorization information applies after users pass authentication:

- Login users obtain the level-0 user role. Login users include the Telnet, FTP, SFTP, SCP, and terminal users. Terminal users can access the device through the console port. For more information about the level-0 user role, see RBAC configuration in *Fundamentals Configuration Guide*.
- The working directory for FTP, SFTP, and SCP login users is the root directory of the NAS. However, the users do not have permission to access the root directory.
- Non-login users can access the network.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

The default authorization method is used for all users that support this method and do not have an authorization method configured.

The RADIUS authorization configuration takes effect only when the authentication method and authorization method of the ISP domain use the same RADIUS scheme.

You can specify one primary authorization method and multiple backup authorization methods.

When the default authorization method is invalid, the device attempts to use the backup authorization methods in sequence. For example, the **authorization default radius-scheme** *radius-scheme-name* **local none** command specifies the default RADIUS authorization method and two backup methods (local authorization and no authorization). The device performs RADIUS authorization by default and performs local authorization when the RADIUS server is invalid. The device does not perform authorization when both of the previous methods are invalid.

Examples

In ISP domain **test**, use RADIUS scheme **rd** as the primary default authorization method and use local authorization as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization default radius-scheme rd local
```

Related commands

hwtacacs scheme

local-user

radius scheme

authorization lan-access

Use **authorization lan-access** to specify authorization methods for LAN users.

Use **undo authorization lan-access** to restore the default.

Syntax

In non-FIPS mode:

authorization lan-access { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authorization lan-access

In FIPS mode:

authorization lan-access { **local** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authorization lan-access

Default

The default authorization methods of the ISP domain are used for LAN users.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

local: Performs local authorization.

none: Does not perform authorization. An authenticated LAN user directly accesses the network.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

The RADIUS authorization configuration takes effect only when authentication and authorization methods of the ISP domain use the same RADIUS scheme.

You can specify one primary authorization method and multiple backup authorization methods.

When the primary method is invalid, the device attempts to use the backup methods in sequence. For example, the **authorization lan-access radius-scheme** *radius-scheme-name* **local none** command specifies a primary RADIUS authorization method and two backup methods (local authorization and no authorization). The device performs RADIUS authorization by default and performs local authorization when the RADIUS server is invalid. The device does not perform authorization when both of the previous methods are invalid.

Examples

In ISP domain **test**, perform local authorization for LAN users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization lan-access local
```

In ISP domain **test**, perform RADIUS authorization for LAN users based on scheme **rd** and use local authorization as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization lan-access radius-scheme rd local
```

Related commands

authorization default

local-user

radius scheme

authorization login

Use **authorization login** to specify authorization methods for login users.

Use **undo authorization login** to restore the default.

Syntax

In non-FIPS mode:

authorization login { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }

undo authorization login

In FIPS mode:

authorization login { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] | **local** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] }

undo authorization login

Default

The default authorization methods of the ISP domain are used for login users.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local authorization.

none: Does not perform authorization. The following default authorization information applies after users pass authentication:

- Login users obtain the level-0 user role. Login users include the Telnet, FTP, SFTP, SCP, and terminal users. Terminal users can access the device through the console port. For more information about the level-0 user role, see RBAC configuration in *Fundamentals Configuration Guide*.
- The working directory for FTP, SFTP, and SCP login users is the root directory of the NAS. However, the users do not have permission to access the root directory.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

The RADIUS authorization configuration takes effect only when the authentication method and authorization method of the ISP domain use the same RADIUS scheme.

You can specify one primary authorization method and multiple backup authorization methods.

When the default authorization method is invalid, the device attempts to use the backup authorization methods in sequence. For example, the **authorization login radius-scheme** *radius-scheme-name* **local none** command specifies the default RADIUS authorization method and two backup methods (local authorization and no authorization). The device performs RADIUS authorization by default and performs local authorization when the RADIUS server is invalid. The device does not perform authorization when both of the previous methods are invalid.

Examples

In ISP domain **test**, perform local authorization for login users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization login local
```

In ISP domain **test**, perform RADIUS authorization for login users based on scheme **rd** and use local authorization as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization login radius-scheme rd local
```

Related commands

authorization default

hwtacacs scheme

local-user

radius scheme

authorization portal

Use **authorization portal** to specify authorization methods for portal users.

Use **undo authorization portal** to restore the default.

Syntax

In non-FIPS mode:

authorization portal { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authorization portal

In FIPS mode:

authorization portal { **local** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authorization portal

Default

The default authorization methods of the ISP domain are used for portal users.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

local: Performs local authorization.

none: Does not perform authorization. An authenticated portal user directly accesses the network.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

The RADIUS authorization configuration takes effect only when the authentication method and authorization method of the ISP domain use the same RADIUS scheme.

You can specify one primary authorization method and multiple backup authorization methods.

When the default authorization method is invalid, the device attempts to use the backup authorization methods in sequence. For example, the **authorization portal radius-scheme** *radius-scheme-name* **local none** command specifies the default RADIUS authorization method and two backup methods (local authorization and no authorization). The device performs RADIUS authorization by default and performs local authorization when the RADIUS server is invalid. The device does not perform authorization when both of the previous methods are invalid.

Examples

In ISP domain **test**, perform local authorization for portal users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization portal local
```

In ISP domain **test**, perform RADIUS authorization for portal users based on scheme **rd** and use local authorization as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization portal radius-scheme rd local
```

Related commands

authorization default

local-user

radius scheme

authorization-attribute (ISP domain view)

Use **authorization-attribute** to configure authorization attributes for users in an ISP domain.

Use **undo authorization-attribute** to restore the default of an authorization attribute.

Syntax

authorization-attribute { **acl** *acl-number* | **car inbound cir** *committed-information-rate* [**pir** *peak-information-rate*] **outbound cir** *committed-information-rate* [**pir** *peak-information-rate*] | **igmp max-access-number** *max-access-number* | **ip-pool** *ipv4-pool-name* | **ipv6-pool** *ipv6-pool-name* | **mld max-access-number** *max-access-number* | **url** *url-string* | **user-group** *user-group-name* | **user-profile** *profile-name* }

undo authorization-attribute { **acl** | **car** | **igmp** | **ip-pool** | **ipv6-pool** | **mld** | **url** | **user-group** | **user-profile** }

Default

An IPv4 user can concurrently join a maximum of four IGMP multicast groups.

An IPv6 user can concurrently join a maximum of four MLD multicast groups.

No other authorization attributes exist.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

acl *acl-number*: Specifies an ACL to filter traffic for users. The value range for the *acl-number* argument is 2000 to 4999. This option is applicable only to portal and LAN users. The device processes the traffic that matches the rules in the authorization ACL based on the permit or deny statement in the rules.

car: Specifies a CAR action for users. Typically, the attribute applies to authenticated users. If you configure the attribute in a portal preauthentication domain, the CAR action applies before portal authentication. This keyword is applicable only to portal users.

inbound: Specifies the upload rate of users.

outbound: Specifies the download rate of users.

cir *committed-information-rate*: Specifies the committed information rate in kbps, in the range of 1 to 4194303.

pir *peak-information-rate*: Specifies the peak information rate in kbps, in the range of 1 to 4194303. The peak information rate cannot be smaller than the committed information rate. If you do not specify this option, the CAR action does not restrict users by peak information rate.

igmp max-access-number *max-access-number*: Specifies the maximum number of IGMP groups that an IPv4 user can join concurrently. The value range for the *max-access-number* argument is 1 to 64. This option is applicable only to portal users.

ip-pool *ipv4-pool-name*: Specifies an IPv4 address pool for users. The *ipv4-pool-name* argument is a case-insensitive string of 1 to 63 characters. This option is applicable only to portal users.

ipv6-pool *ipv6-pool-name*: Specifies an IPv6 address pool for users. The *ipv6-pool-name* argument is a case-insensitive string of 1 to 63 characters. This option is applicable only to portal users.

mld max-access-number *max-access-number*: Specifies the maximum number of MLD groups that an IPv6 user can join concurrently. The value range for the *max-access-number* argument is 1 to 64. This option is applicable only to portal users.

url *url-string*: Specifies a redirect URL for users. Users are redirected to the URL the first time they access the network after they pass authentication. The *url-string* argument is a case-sensitive string of 1 to 255 characters. This option is applicable only to LAN users.

user-group *user-group-name*: Specifies a user group for users. The *user-group-name* argument is a case-insensitive string of 1 to 32 characters. Authenticated users obtain all attributes of the user group.

user-profile *profile-name*: Specifies an authorization user profile. The *profile-name* argument is a case-sensitive string of 1 to 31 characters. Typically, the attribute applies to authenticated users. If you configure the attribute in a portal preauthentication domain, the user profile applies before portal authentication. This option is applicable only to portal and LAN users.

Usage guidelines

If the server or NAS does not authorize a type of attribute to an authenticated user, the device authorizes the attribute in the ISP domain to the user.

You can configure multiple authorization attributes for users in an ISP domain. If you execute the command multiple times with the same attribute specified, the most recent configuration takes effect.

For portal users to come online after passing authentication, make sure ACLs assigned to portal users do not have rules specified with a source IP or MAC address.

Examples

Specify user group **abc** as the authorization user group for users in ISP domain **test**.

```
<Sysname> system-view
```

```
[Sysname] domain test
[Sysname-isp-test] authorization-attribute user-group abc
```

Related commands

display domain

display domain

Use **display domain** to display ISP domain configuration.

Syntax

display domain [*isp-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

isp-name: Specifies an ISP domain by its name, a case-insensitive string of 1 to 255 characters. If you do not specify an ISP domain, this command displays the configuration of all ISP domains.

Examples

Display the configuration of all ISP domains.

```
<Sysname> display domain
Total 2 domains

Domain: system
  State: Active
  Default authentication scheme:  Local
  Default authorization  scheme:  Local
  Default accounting     scheme:  Local
  Accounting start failure action: Online
  Accounting update failure action: Online
  Accounting quota out policy: Offline
  Service type: HSI
  Session time: Exclude idle time
  Dual-stack accounting method: Merge
  Authorization attributes:
    Idle cut: Disabled
    IGMP access limit: 4
    MLD access limit: 4

Domain: dm
  State: Active
  Login   authentication scheme:  RADIUS=rad
  Login   authorization  scheme:  HWTACACS=hw
  Super   authentication scheme:  RADIUS=rad
  Command authorization  scheme:  HWTACACS=hw
```

```
  LAN access authentication scheme:  RADIUS=r4
  Portal  authentication scheme:  LDAP=ldp
  Default authentication scheme:  RADIUS=rad, Local, None
  Default authorization  scheme:  Local
  Default accounting     scheme:  None
  Accounting start failure action: Online
  Accounting update failure action: Online
  Accounting quota out policy: Offline
  Service type: HSI
  Session time: Include idle time
  Dual-stack accounting method: Merge
  Authorization attributes:
    Idle cut : Disabled
    IP pool: appy
    User profile: test
    Inbound CAR: CIR 64000 bps PIR 640000 bps
    Outbound CAR: CIR 64000 bps PIR 640000 bps
    ACL number: 3000
    User group: ugg
    IPv6 pool: ipv6pool
    URL: http://test
    IGMP access limit: 4
    MLD access limit: 4

Default domain name: system
```

Table 1 Command output

Field	Description
Domain	ISP domain name.
State	Status of the ISP domain.
Default authentication scheme	Default authentication methods.
Default authorization scheme	Default authorization methods.
Default accounting scheme	Default accounting methods.
Login authentication scheme	Authentication methods for login users.
Login authorization scheme	Authorization methods for login users.
Login accounting scheme	Accounting methods for login users.
Super authentication scheme	Authentication methods for obtaining another user role without reconnecting to the device.
Command authorization scheme	Command line authorization methods.
Command accounting scheme	Command line accounting method.
LAN access authentication scheme	Authentication methods for LAN users.
LAN access authorization scheme	Authorization methods for LAN users.
LAN access accounting scheme	Accounting methods for LAN users.
Portal authentication scheme	Authentication methods for portal users.

Field	Description
Portal authorization scheme	Authorization methods for portal users.
Portal accounting scheme	Accounting methods for portal users.
RADIUS	RADIUS scheme.
HWTACACS	HWTACACS scheme.
LDAP	LDAP scheme.
Local	Local scheme.
None	No authentication, no authorization, or no accounting.
Accounting start failure action	Access control for users that encounter accounting-start failures: • **Online**—Allows the users to stay online. • **Offline**—Logs off the users.
Accounting update failure max-times	Maximum number of consecutive accounting-update failures allowed by the device for each user in the domain.
Accounting update failure action	Access control for users that have failed all their accounting-update attempts: • **Online**—Allows the users to stay online. • **Offline**—Logs off the users.
Accounting quota out policy	Access control for users that have used up their accounting quotas: • **Online**—Allows the users to stay online. • **Offline**—Logs off the users.
Service type	This field is not supported in the current software version. Service type of the ISP domain, including HSI, STB, and VoIP.
Session time	Online duration sent to the server for users that went offline due to connection failure or malfunction: • **Include idle time**—The online duration includes the idle timeout period. • **Exclude idle time**—The online duration does not include the idle timeout period.
Dual-stack accounting method	This field is not supported in the current software version. Accounting method for dual-stack users: • **Merge**—Merges IPv4 data with IPv6 data for accounting. • **Separate**—Separates IPv4 data from IPv6 data for accounting.
Authorization attributes	Authorization attributes for users in the ISP domain.
Idle cut	This field is not supported in the current software version. Idle cut feature status: • **Enabled**—The feature is enabled. The device logs off users that do not meet the minimum traffic requirements in an idle timeout period. • **Disabled**—The feature is disabled. It is the default idle cut state.
Idle timeout	Idle timeout period, in minutes.
Flow	Minimum traffic that a login user must generate in an idle timeout period, in bytes.
Traffic direction	Traffic direction for the idle cut feature:

Field	Description
	• **Both**. • **Inbound**. • **Outbound**.
IP pool	Name of the authorization IPv4 address pool.
User profile	Name of the authorization user profile.
Inbound CAR	Authorization inbound CAR: • **CIR**—Committed information rate in bps. • **PIR**—Peak information rate in bps. If no inbound CAR is authorized, this field displays **N/A**.
Outbound CAR	Authorization outbound CAR: • **CIR**—Committed information rate in bps. • **PIR**—Peak information rate in bps. If no outbound CAR is authorized, this field displays **N/A**.
ACL number	Authorization ACL for users.
User group	Authorization user group for users.
IPv6 pool	Name of the authorization IPv6 address pool for users.
URL	Authorization redirect URL for users.
IGMP access limit	Maximum number of IGMP groups that an IPv4 user is authorized to join concurrently.
MLD access limit	Maximum number of MLD groups that an IPv6 user is authorized to join concurrently.

domain

Use **domain** to create an ISP domain and enter its view, or enter the view of an existing ISP domain.

Use **undo domain** to delete an ISP domain.

Syntax

domain *isp-name*

undo domain *isp-name*

Default

A system-defined ISP domain exists. The domain name is **system**.

Views

System view

Predefined user roles

network-admin

Parameters

isp-name: Specifies the ISP domain name, a case-insensitive string of 1 to 255 characters. The name must meet the following requirements:

- The name cannot contain a forward slash (/), backslash (\), vertical bar (|), quotation marks ("), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@).

- The name cannot be **d**, **de**, **def**, **defa**, **defau**, **defaul**, **default**, **i**, **if**, **if-**, **if-u**, **if-un**, **if-unk**, **if-unkn**, **if-unkno**, **if-unknow**, or **if-unknown**.

Usage guidelines

All ISP domains are in active state when they are created.

You can modify settings for the system-defined ISP domain **system**, but you cannot delete this domain.

An ISP domain cannot be deleted when it is the default ISP domain. Before you use the **undo domain** command, change the domain to a non-default ISP domain by using the **undo domain default enable** command.

Use short domain names to ensure that user names containing a domain name do not exceed the maximum name length required by different types of users.

Examples

Create an ISP domain named **test** and enter ISP domain view.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test]
```

Related commands

display domain

domain default enable

domain if-unknown

state (ISP domain view)

domain default enable

Use **domain default enable** to specify the default ISP domain. Users without any domain name included in the usernames are considered in the default domain.

Use **undo domain default enable** to restore the default.

Syntax

domain default enable *isp-name*

undo domain default enable

Default

The default ISP domain is the system-defined ISP domain **system**.

Views

System view

Predefined user roles

network-admin

Parameters

isp-name: Specifies the ISP domain name, a case-insensitive string of 1 to 255 characters. The ISP domain must already exist.

Usage guidelines

The system has only one default ISP domain.

An ISP domain cannot be deleted when it is the default ISP domain. Before you use the **undo domain** command, change the domain to a non-default ISP domain by using the **undo domain default enable** command.

Examples

Create an ISP domain named **test**, and configure the domain as the default ISP domain.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] quit
[Sysname] domain default enable test
```

Related commands

display domain

domain

domain if-unknown

Use **domain if-unknown** to specify an ISP domain to accommodate users that are assigned to nonexistent domains.

Use **undo domain if-unknown** to restore the default.

Syntax

domain if-unknown *isp-name*

undo domain if-unknown

Default

No ISP domain is specified to accommodate users that are assigned to nonexistent domains.

Views

System view

Predefined user roles

network-admin

Parameters

isp-name: Specifies the ISP domain name, a case-insensitive string of 1 to 255 characters. The name must meet the following requirements:

- The name cannot contain a forward slash (/), backslash (\), vertical bar (|), quotation marks ("), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@).
- The name cannot be **d**, **de**, **def**, **defa**, **defau**, **defaul**, **default**, **i**, **if**, **if-**, **if-u**, **if-un**, **if-unk**, **if-unkn**, **if-unkno**, **if-unknow**, or **if-unknown**.

Usage guidelines

The device chooses an authentication domain for each user in the following order:

1. The authentication domain specified for the access module.
2. The ISP domain in the username.
3. The default ISP domain of the device.

If the chosen domain does not exist on the device, the device searches for the ISP domain that accommodates users assigned to nonexistent domains. If no such ISP domain is configured, user authentication fails.

NOTE:

Support for the authentication domain configuration depends on the access module.

Examples

Specify ISP domain **test** to accommodate users that are assigned to nonexistent domains.

```
<Sysname> system-view
[Sysname] domain if-unknown test
```

Related commands

display domain

local-server log change-password-prompt

Use **local-server log change-password-prompt** to enable password change prompt logging.

Use **undo local-server log change-password-prompt** to disable password change prompt logging.

Syntax

local-server log change-password-prompt

undo local-server log change-password-prompt

Default

Password change prompt logging is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command is supported only in Release 6318P01 and later.

Use this feature to enhance the protection of passwords for Telnet, SSH, HTTP, HTTPS, NETCONF over SSH, and NETCONF over SOAP users and improve the system security.

This feature enables the device to generate logs to prompt users to change their weak passwords at an interval of 24 hours and at the users' login.

A password is a weak password if it does not meet the following requirements:

- Password composition restriction configured by using the **password-control composition** command.
- Minimum password length restriction set by using the **password-control length** command.
- It cannot contain the username or the reverse letters of the username.

For a NETCONF over SSH or NETCONF over SOAP user, the device also generates a password change prompt log if any of the following conditions exists:

- The current password of the user is the default password or has expired.
- The user logs in to the device for the first time or uses a new password to log in after global password control is enabled.

The device will no longer generate password change prompt logs for a user when one of the following conditions exists:

- The password change prompt logging feature is disabled.
- The user has changed the password and the new password meets the password control requirements.
- The enabling status of a related password control feature has changed so the current password of the user meets the password control requirements.
- The password composition policy or the minimum password length has changed.

You can use the **display password-control** command to display password control configuration. For more information about password control commands, see "Password control commands."

Examples

Enable password change prompt logging.

```
<Sysname> system-view
[Sysname] local-server log change-password-prompt
```

Related commands

display password-control

password-control composition

password-control length

nas-id bind vlan

Use **nas-id bind vlan** to bind a NAS-ID with a VLAN.

Use **undo nas-id bind vlan** to remove a NAS-ID and VLAN binding.

Syntax

nas-id *nas-identifier* **bind vlan** *vlan-id*

undo nas-id *nas-identifier* **bind vlan** *vlan-id*

Default

No NAS-ID and VLAN bindings exist.

Views

NAS-ID profile view

Predefined user roles

network-admin

Parameters

nas-identifier: Specifies a NAS-ID, a case-sensitive string of 1 to 31 characters.

vlan-id: Specifies a VLAN ID in the range of 1 to 4094.

Usage guidelines

You can configure multiple NAS-ID and VLAN bindings in a NAS-ID profile.

A NAS-ID can be bound with more than one VLAN, but a VLAN can be bound with only one NAS-ID. If you configure multiple bindings for the same VLAN, the most recent configuration takes effect.

Examples

Bind NAS-ID 222 with VLAN 2 in NAS-ID profile **aaa**.

```
<Sysname> system-view
[Sysname] aaa nas-id profile aaa
[Sysname-nas-id-prof-aaa] nas-id 222 bind vlan 2
```

Related commands

aaa nas-id profile

session-time include-idle-time

Use **session-time include-idle-time** to configure the device to include the idle timeout period in the user online duration sent to the server.

Use **undo session-time include-idle-time** to restore the default.

Syntax

session-time include-idle-time

undo session-time include-idle-time

Default

The device does not include the idle timeout period in the user online duration sent to the server.

Views

ISP domain view

Predefined user roles

network-admin

Usage guidelines

Whether to configure the device to include the idle timeout period in the user online duration sent to the server, depending on the accounting policy in your network. The idle timeout period is assigned to users by the authorization server after the users pass authentication. For portal users, the device includes the idle timeout period set for the online portal user detection feature in the user online duration. For more information about online detection for portal users, see portal authentication configuration in *Security Configuration Guide*.

If the user goes offline due to connection failure or malfunction, the user online duration sent to the server is not the same as the actual online duration.

- If the **session-time include-idle-time** command is used, the user's online duration sent to the server includes the idle timeout period. The online duration that is generated on the server is longer than the actual online duration of the user.
- If the **undo session-time include-idle-time** command is used, the user's online duration sent to the server excludes the idle timeout period. The online duration that is generated on the server is shorter than the actual online duration of the user.

Examples

Configure the device to include the idle timeout period in the online duration sent to the server for users in ISP domain **test**.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] session-time include-idle-time
```

Related commands

display domain

state (ISP domain view)

Use **state** to set the status of an ISP domain.

Use **undo state** to restore the default.

Syntax

state { **active** | **block** }

undo state

Default

An ISP domain is in active state.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

active: Places the ISP domain in active state to allow the users in the ISP domain to request network services.

block: Places the ISP domain in blocked state to prevent users in the ISP domain from requesting network services.

Usage guidelines

By blocking an ISP domain, you disable offline users of the domain from requesting network services. However, the online users are not affected.

Examples

Place ISP domain **test** in blocked state.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] state block
```

Related commands

display domain

Local user commands

access-limit

Use **access-limit** to set the maximum number of concurrent logins using the local user name.

Use **undo access-limit** to restore the default.

Syntax

access-limit *max-user-number*

undo access-limit

Default

The number of concurrent logins using the local user name is not limited.

Views

Local user view

Predefined user roles

network-admin

Parameters

max-user-number: Specifies the maximum number of concurrent logins, in the range of 1 to 1024.

Usage guidelines

This command takes effect only when local accounting is configured for the local user. The command does not apply to FTP, SFTP, or SCP users. These users do not support accounting.

For this command to take effect on network access users, you also need to execute the **accounting start-fail offline** command in the ISP domain view.

Examples

Set the maximum number of concurrent logins to 5 for users using the local user name **abc**.

```
<Sysname> system-view
[Sysname] local-user abc
[Sysname-luser-manage-abc] access-limit 5
```

Related commands

accounting start-fail offline

display local-user

authorization-attribute (local user view/user group view)

Use **authorization-attribute** to configure authorization attributes for a local user or user group. After the local user or a local user in the user group passes authentication, the device assigns these attributes to the user.

Use **undo authorization-attribute** to restore the default of an authorization attribute.

Syntax

authorization-attribute { **acl** *acl-number* | **idle-cut** *minutes* | **ip-pool** *ipv4-pool-name* | **ipv6-pool** *ipv6-pool-name* | **session-timeout** *minutes* | **user-profile** *profile-name* | **user-role** *role-name* | **vlan** *vlan-id* | **work-directory** *directory-name* } *

undo authorization-attribute { **acl** | **idle-cut** | **ip-pool** | **ipv6-pool** | **session-timeout** | **user-profile** | **user-role** *role-name* | **vlan** | **work-directory** } *

Default

The working directory for FTP, SFTP, and SCP users is the root directory of the NAS. However, the users do not have permission to access the root directory.

The local users created by a network-admin or level-15 user are assigned the network-operator user role.

Views

Local user view

User group view

Predefined user roles

network-admin

Parameters

acl *acl-number*: Specifies an authorization ACL. The value range for the *acl-number* argument is 2000 to 4999. The device processes the traffic that matches the rules in the authorization ACL based on the permit or deny statement in the rules.

idle-cut *minutes*: Specifies an idle timeout period in minutes. The value range for the *minutes* argument is 1 to 120. An online user is logged out if its idle period exceeds the specified idle timeout period.

ip-pool *ipv4-pool-name*: Specifies an IPv4 address pool for the user. The *ipv4-pool-name* argument is a case-insensitive string of 1 to 63 characters.

ipv6-pool *ipv6-pool-name*: Specifies an IPv6 address pool for the user. The *ipv6-pool-name* argument is a case-insensitive string of 1 to 63 characters.

session-timeout *minutes*: Specifies the session timeout timer for the user, in minutes. The value range for the *minutes* argument is 1 to 1440. The device logs off the user after the timer expires.

user-profile *profile-name*: Specifies an authorization user profile by its name. The *profile-name* argument is a case-sensitive string of 1 to 31 characters. The name can contain only letters, digits, and underscores (_). The user profile restricts the behavior of authenticated users. For more information, see *Security Configuration Guide*.

user-role *role-name*: Specifies an authorized user role. The *role-name* argument is a case-sensitive string of 1 to 63 characters. A maximum of 64 user roles can be specified for a user. For user role-related commands, see *Fundamentals Command Reference* for RBAC commands. This option is available only in local user view, and is not available in user group view.

vlan *vlan-id*: Specifies an authorized VLAN. The value range for the *vlan-id* argument is 1 to 4094. After passing authentication and being authorized a VLAN, a local user can access only the resources in this VLAN.

work-directory *directory-name*: Specifies the working directory for FTP, SFTP, or SCP users. The *directory-name* argument is a case-insensitive string of 1 to 255 characters. The directory must already exist.

Usage guidelines

Configure authorization attributes according to the application environments and purposes. Support for authorization attributes depends on the service types of users.

For portal users, only the following authorization attributes take effect: **acl**, **ip-pool**, **ipv6-pool**, **user-profile**, and **session-timeout**.

For LAN users, only the following authorization attributes take effect: **acl**, **session-timeout**, **user-profile**, and **vlan**.

For SSH, Telnet, and terminal users, only the authorization attributes **idle-cut** and **user-role** take effect.

For HTTP and HTTPS users, only the authorization attribute **user-role** takes effect.

For FTP users, only the authorization attributes **user-role** and **work-directory** take effect.

For other types of local users, no authorization attribute takes effect.

Authorization attributes configured for a user group are intended for all local users in the group. You can group local users to improve configuration and management efficiency. An authorization attribute configured in local user view takes precedence over the same attribute configured in user group view.

For portal users to come online after passing authentication, make sure ACLs assigned to portal users do not have rules specified with a source IP or MAC address.

To make sure FTP, SFTP, and SCP users can access the directory after an IRF master/subordinate switchover, do not specify slot information for the working directory.

To make sure the user have only the user roles authorized by using this command, use the **undo authorization-attribute user-role** command to remove the default user role.

The security-audit user role has access to the commands for managing security log files and security log file system. To display all the accessible commands of the security-audit user role, use the **display role name security-audit** command. For more information about security log management, see *Network Management and Monitoring Configuration Guide*. For more information about file system management, see *Fundamentals Configuration Guide*.

You cannot delete a local user if the local user is the only user that has the security-audit user role.

The security-audit user role is mutually exclusive with other user roles.

- When you assign the security-audit user role to a local user, the system requests confirmation for deleting all the other user roles of the user.
- When you assign other user roles to a local user that has the security-audit user role, the system requests confirmation for deleting the security-audit user role for the local user.

Examples

Configure the authorized VLAN of network access user **abc** as VLAN 2.

```
<Sysname> system-view
[Sysname] local-user abc class network
[Sysname-luser-network-abc] authorization-attribute vlan 2
```

Configure the authorized VLAN of user group **abc** as VLAN 3.

```
<Sysname> system-view
[Sysname] user-group abc
[Sysname-ugroup-abc] authorization-attribute vlan 3
```

Assign the **security-audit** user role to device management user **xyz** as the authorized user role.

```
<Sysname> system-view
[Sysname] local-user xyz class manage
[Sysname-luser-manage-xyz] authorization-attribute user-role security-audit
This operation will delete all other roles of the user. Are you sure? [Y/N]:y
```

Related commands

display local-user

display user-group

bind-attribute

Use **bind-attribute** to configure binding attributes for a local user.

Use **undo bind-attribute** to remove binding attributes of a local user.

Syntax

bind-attribute { **ip** *ip-address* | **location interface** *interface-type interface-number* | **mac** *mac-address* | **vlan** *vlan-id* } *

undo bind-attribute { **ip** | **location** | **mac** | **vlan** } *

Default

No binding attributes are configured for a local user.

Views

Local user view

Predefined user roles

network-admin

Parameters

ip *ip-address*: Specifies the IP address to which the user is bound. This option applies only to 802.1X users.

location interface *interface-type interface-number*: Specifies the interface to which the user is bound. The *interface-type* argument represents the interface type, and the *interface-number* argument represents the interface number. To pass authentication, the user must access the network through the bound interface. This option applies only to device management, LAN, and portal users.

mac *mac-address*: Specifies the MAC address of the user in the format H-H-H. This option applies only to LAN and portal users.

vlan *vlan-id*: Specifies the VLAN to which the user belongs. The *vlan-id* argument is in the range of 1 to 4094. This option applies only to LAN and portal users.

Usage guidelines

To perform local authentication of a user, the device matches the actual user attributes with the configured binding attributes. If the user has a non-matching attribute or lacks a required attribute, the user will fail authentication.

Binding attribute check takes effect on all access services. Configure the binding attributes for a user based on the access services and make sure the device can obtain all attributes to be checked from the user's packet. For example, you can configure an IP address binding for an 802.1X user, because 802.1X authentication can include the user's IP address in the packet. However, you cannot configure IP address bindings for MAC authentication users, because MAC authentication does not use IP addresses.

The binding interface type must meet the requirements of the local user. Configure the binding interface based on the service type of the user.

- If the user is an 802.1X user, specify the 802.1X-enabled Layer 2 Ethernet interface.
- If the user is a MAC authentication user, specify the MAC authentication-enabled Layer 2 Ethernet interface.
- If the user is a Web authentication user, specify the Web authentication-enabled Layer 2 Ethernet interface.
- If the user is a portal user, specify the portal-enabled interface. Specify the Layer 2 Ethernet interface if portal is enabled on a VLAN interface and the **portal roaming enable** command is not configured.

Examples

Bind MAC address 11-11-11 with network access user **abc**.

```
<Sysname> system-view
[Sysname] local-user abc class network
[Sysname-luser-network-abc] bind-attribute mac 11-11-11
```

Related commands

display local-user

description

Use **description** to configure a description for a network access user.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

No description is configured for a network access user.

Views

Network access user view

Predefined user roles

network-admin

Parameters

text: Configures a description, case-sensitive string of 1 to 255 characters.

Examples

Configure a description for network access user **123**.

```
<Sysname> system-view
[Sysname] local-user 123 class network
[Sysname-luser-network-123] description Manager of MSC company
```

Related commands

display local-user

display local-user

Use **display local-user** to display the local user configuration and online user statistics.

Syntax

display local-user [**class** { **manage** | **network** } | **idle-cut** { **disable** | **enable** } | **service-type** { **ftp** | **http** | **https** | **lan-access** | **portal** | **ssh** | **telnet** | **terminal** } | **state** { **active** | **block** } | **user-name** *user-name* **class** { **manage** | **network** } | **vlan** *vlan-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

class: Specifies the local user type.

manage: Device management user.

network: Network access user.

idle-cut { **disable** | **enable** }: Specifies local users by the status of the idle cut feature.

service-type: Specifies the local users that use a specific type of service.

ftp: FTP users.

http: HTTP users.

https: HTTPS users.

lan-access: LAN users that typically access the network through an Ethernet, such as 802.1X users.

portal: Portal users.

ssh: SSH users.

telnet: Telnet users.

terminal: Terminal users that log in through console ports.

state { **active** | **block** }: Specifies local users in active or blocked state. A local user in active state can access network services, but a local user in blocked state cannot.

user-name *user-name*: Specifies all local users using the specified username. The username must be a case-sensitive string of 1 to 55 characters. The name must meet the following requirements:

- Cannot contain the domain name.
- Cannot contain any of the following characters: forward slash (/), backslash (\), vertical bar (|), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@).
- Cannot be **a**, **al**, or **all**.

vlan *vlan-id*: Specifies all local users in a VLAN. The *vlan-id* argument is in the range of 1 to 4094.

Usage guidelines

If you do not specify any parameters, this command displays information about all local users.

Examples

Display information about all local users.

```
<Sysname> display local-user
Device management user root:
  State:                     Active
  Service type:              SSH/Telnet/Terminal
  Access limit:              Enabled           Max access number: 3
  Current access number:     1
  User group:                system
  Bind attributes:
  Authorization attributes:
    Work directory:          flash:
    User role list:          network-admin
  Password control configurations:
    Password aging:          3 days
  Password history was last reset: 0 days ago

Network access user jj:
  State:                      Active
```

```
  Service type:               LAN-access
  User group:                 system
  Bind attributes:
    IP address:               2.2.2.2
    Location bound:           GigabitEthernet1/0/1
    MAC address:              0001-0001-0001
    VLAN ID:                  2
  Authorization attributes:
    Idle timeout:             33 minutes
    Work directory:           flash:
    ACL number:               2000
    User profile:               pp
    User role list:             network-operator, level-0, level-3
  Description:                A network access user from company cc
  Validity period:
    Start date and time:      2016/01/01-00:01:01
    Expiration date and time: 2017/01/01-01:01:01
  Password control configurations:
    Password length:          4 characters

Total 2 local users matched.
```

Table 2 Command output

Field	Description
State	Status of the local user: active or blocked.
Service type	Service types that the local user can use.
Access limit	Whether the concurrent login limit is enabled.
Max access number	Maximum number of concurrent logins using the local user name.
Current access number	Current number of concurrent logins using the local user name.
User group	Group to which the local user belongs.
Bind attributes	Binding attributes of the local user.
IP address	IP address of the local user.
Location bound	Binding port of the local user.
MAC address	MAC address of the local user.
VLAN ID	Binding VLAN of the local user.
Authorization attributes	Authorization attributes of the local user.
Idle timeout	Idle timeout period of the user, in minutes.
Session-timeout	Session timeout timer for the user, in minutes.
Work directory	Directory that the FTP, SFTP, or SCP user can access.
ACL number	Authorization ACL of the local user.
VLAN ID	Authorized VLAN of the local user.
User profile	Authorization user profile of the local user.
User role list	Authorized roles of the local user.

Field	Description
IP pool	IPv4 address pool authorized to the local user.
IPv6 pool	IPv6 address pool authorized to the local user.
Password control configurations	Password control attributes that are configured for the local user.
Password aging	Password expiration time.
Password length	Minimum number of characters that a password must contain.
Password composition	Password composition policy: • Minimum number of character types that a password must contain. • Minimum number of characters from each type in a password.
Password complexity	Password complexity checking policy: • Reject a password that contains the username or the reverse of the username. • Reject a password that contains any character repeated consecutively three or more times.
Maximum login attempts	Maximum number of consecutive failed login attempts.
Action for exceeding login attempts	Action to take on the user that failed to log in after using up all login attempts.
Password history was last reset	The most recent time that the history password records were cleared.
Description	Description of the network access user.
Validity period	Validity period of the network access user.
Start date and time	Date and time from which the network access user begins to take effect.
Expiration date and time	Date and time at which the network access user expires.

display user-group

Use **display user-group** to display user group configuration.

Syntax

display user-group { **all** | **name** *group-name* }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

all: Specifies all user groups.

name *group-name*: Specifies a user group by its name, a case-insensitive string of 1 to 32 characters.

Examples

Display the configuration of all user groups.

```
<Sysname> display user-group all
```

```
Total 2 user groups matched.

User group: system
  Authorization attributes:
    Work directory:          flash:
User group: jj
  Authorization attributes:
    Idle timeout:            2 minutes
    Work directory:          flash:/
    ACL number:              2000
    VLAN ID:                 2
    User profile:            pp
  Password control configurations:
    Password aging:          2 days
```

Table 3 Command output

Field	Description
User group	User group name.
Authorization attributes	Authorization attributes of the user group.
Idle timeout	Idle timeout period, in minutes.
Session-timeout	Session timeout timer, in minutes.
Work directory	Directory that FTP, SFTP, or SCP users in the group can access.
ACL number	Authorization ACL.
VLAN ID	Authorized VLAN.
User profile	Authorization user profile.
IP pool	IPv4 address pool authorized to the user group.
IPv6 pool	IPv6 address pool authorized to the user group.
Password control configurations	Password control attributes that are configured for the user group.
Password aging	Password expiration time.
Password length	Minimum number of characters that a password must contain.
Password composition	Password composition policy: • Minimum number of character types that a password must contain. • Minimum number of characters from each type in a password.
Password complexity	Password complexity checking policy: • Reject a password that contains the username or the reverse of the username. • Reject a password that contains any character repeated consecutively three or more times.
Maximum login attempts	Maximum number of consecutive failed login attempts.
Action for exceeding login attempts	Action to take on the user that failed to log in after using up all login attempts.

group

Use **group** to assign a local user to a user group.

Use **undo group** to restore the default.

Syntax

group *group-name*

undo group

Default

A local user belongs to user group **system**.

Views

Local user view

Predefined user roles

network-admin

Parameters

group-name: Specifies the user group name, a case-insensitive string of 1 to 32 characters.

Examples

Assign device management user **111** to user group **abc**.

```
<Sysname> system-view
[Sysname] local-user 111 class manage
[Sysname-luser-manage-111] group abc
```

Related commands

display local-user

local-user

Use **local-user** to add a local user and enter its view, or enter the view of an existing local user.

Use **undo local-user** to delete local users.

Syntax

local-user *user-name* [**class** { **manage** | **network** }]

undo local-user { *user-name* **class** { **manage** | **network** } | **all** [**service-type** { **ftp** | **http** | **https** | **lan-access** | **portal** | **ssh** | **telnet** | **terminal** } | **class** { **manage** | **network** }] }

Default

No local users exist.

Views

System view

Predefined user roles

network-admin

Parameters

user-name: Specifies the local user name, a case-sensitive string of 1 to 55 characters. The name must meet the following requirements:

- Cannot contain a domain name.
- Cannot contain any of the following characters: forward slash (/), backslash (\), vertical bar (|), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@).
- Cannot be a substring of **all** or **auto-delete** that starts with character **a** (for example, **a**, **al**, **all**, **au**, **aut**, **auto**, or **auto-**).

class: Specifies the local user type. If you do not specify this keyword, the command adds a device management user.

manage: Device management user that can configure and monitor the device after login. Device management users can use FTP, HTTP, HTTPS, Telnet, SSH, and terminal services.

network: Network access user that accesses network resources through the device. Network access users can use LAN access and portal services.

all: Specifies all users.

service-type: Specifies the local users that use a specific type of service.

ftp: FTP users.

http: HTTP users.

https: HTTPS users.

lan-access: LAN users that typically access the network through an Ethernet, such as 802.1X users.

portal: Portal users.

ssh: SSH users.

telnet: Telnet users.

terminal: Terminal users that log in through console ports.

Usage guidelines

As from release 6348P01, the factory defaults of the device provide a default local user named **clouduser** of the HTTP type. The user password is **admin** and the user role is **network-admin**. In versions earlier than 6348P01, no default local user is provided.

Examples

Add a device management user named **user1** and enter local user view.

```
<Sysname> system-view
[Sysname] local-user user1 class manage
[Sysname-luser-manage-user1]
```

Add a network access user named **user2** and enter local user view.

```
<Sysname> system-view
[Sysname] local-user user2 class network
[Sysname-luser-network-user2]
```

Related commands

display local-user

service-type

local-user auto-delete enable

Use **local-user auto-delete enable** to enable the local user auto-delete feature.

Use **undo local-user auto-delete enable** to restore the default.

Syntax

local-user auto-delete enable

undo local-user auto-delete enable

Default

The local user auto-delete feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This feature enables the device to examine the validity of local users at fixed time periods of 10 minutes and automatically delete expired local users.

Examples

Enable the local user auto-delete feature.

```
<Sysname> system-view
[Sysname] local-user auto-delete enable
```

Related commands

validity-datetime

password (device management user view)

Use **password** to configure a password for a device management user.

Use **undo password** to restore the default.

Syntax

In non-FIPS mode:

password [{ **hash** | **simple** } *string*]

undo password

In FIPS mode:

password

Default

In non-FIPS mode:

A device management user does not have a password and can pass authentication after entering the correct username and passing attribute checks.

In FIPS mode:

A device management user does not have a password and cannot pass authentication.

Views

Device management user view

Predefined user roles

network-admin

Parameters

hash: Specifies a password encrypted by the hash algorithm.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in hashed form.

string: Specifies the password string. This argument is case sensitive. In non-FIPS mode, the hashed form of the password is a string of 1 to 110 characters. The plaintext form of the password is a string of 1 to 63 characters. In FIPS mode, the password is in plaintext form and is a string of 15 to 63 characters. The string must contain digits, uppercase letters, lowercase letters, and special characters.

Usage guidelines

If you do not specify any parameters, you enter the interactive mode to set a plaintext password.

In non-FIPS mode, a device management user for which no password is specified can pass authentication after entering the correct username and passing attribute checks. To enhance security, configure a password for each device management user.

In FIPS mode, a password is required for a device management user to pass authentication. You must set the password in interactive mode.

When global password control is enabled, the device handles passwords of device management users as follows:

- All passwords in the history records are saved in hashed form.
- If a user changes its own password in plaintext form, the system requests the user to enter the current plaintext password. The new password must be different from all passwords in the history records and the current password. In addition, the new password must have a minimum of four characters different from the current password.
- If a user changes the password for another user in plaintext form, the new password must be different from the latter user's all passwords in the history records and current password.
- If a user deletes its own password, the system requests the user to enter the current plaintext password.
- Except the above listed situations, the system does not request a user to enter the current plaintext password or compare the new password with passwords in the history records and the current password.

Examples

Set the password to **123456TESTplat&!** in plaintext form for device management user **user1**.

```
<Sysname> system-view
[Sysname] local-user user1 class manage
[Sysname-luser-manage-user1] password simple 123456TESTplat&!
```

Configure the password in interactive mode for device management user **test**.

```
<Sysname> system-view
[Sysname] local-user test class manage
[Sysname-luser-manage-test] password
Password:
confirm :
```

Related commands

display local-user

password (network access user view)

Use **password** to configure a password for a network access user.

Use **undo password** to restore the default.

Syntax

password { **cipher** | **simple** } *string*

undo password

Default

A network access user does not have a password and can pass authentication after entering the correct username and passing attribute checks.

Views

Network access user view

Predefined user roles

network-admin

Parameters

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password string. Its plaintext form is a case-sensitive string of 1 to 63 characters. Its encrypted form is a case-sensitive string of 1 to 117 characters.

Usage guidelines

As a best practice to enhance security, configure a password for each network access user.

Examples

Set the password to **123456TESTuser&!** in plaintext form for network access user **user1**.

```
<Sysname> system-view
[Sysname] local-user user1 class network
[Sysname-luser-network-user1] password simple 123456TESTuser&!
```

Related commands

display local-user

service-type

Use **service-type** to specify the service types that a local user can use.

Use **undo service-type** to remove service types configured for a local user.

Syntax

In non-FIPS mode:

service-type { **ftp** | **lan-access** | { **http** | **https** | **ssh** | **telnet** | **terminal** } * | **portal** }

undo service-type { **ftp** | **lan-access** | { **http** | **https** | **ssh** | **telnet** | **terminal** } * | **portal** }

In FIPS mode:

service-type { **lan-access** | { **https** | **ssh** | **terminal** } * | **portal** }

undo service-type { **lan-access** | { **https** | **ssh** | **terminal** } * | **portal** }

Default

A local user is not authorized to use any service.

Views

Local user view

Predefined user roles

network-admin

Parameters

ftp: Authorizes the user to use the FTP service. The authorized directory can be modified by using the **authorization-attribute work-directory** command.

http: Authorizes the user to use the HTTP service.

https: Authorizes the user to use the HTTPS service.

lan-access: Authorizes the user to use the LAN access service. The users are typically Ethernet users, for example, 802.1X users.

ssh: Authorizes the user to use the SSH service.

telnet: Authorizes the user to use the Telnet service.

terminal: Authorizes the user to use the terminal service and log in from a console port.

portal: Authorizes the user to use the portal service.

Usage guidelines

You can assign multiple service types to a user.

Examples

Authorize device management user **user1** to use the Telnet and FTP services.

```
<Sysname> system-view
[Sysname] local-user user1 class manage
[Sysname-luser-manage-user1] service-type telnet
[Sysname-luser-manage-user1] service-type ftp
```

Related commands

display local-user

state (local user view)

Use **state** to set the status of a local user.

Use **undo state** to restore the default.

Syntax

state { **active** | **block** }

undo state

Default

A local user is in active state.

Views

Local user view

Predefined user roles

network-admin

Parameters

active: Places the local user in active state to allow the local user to request network services.

block: Places the local user in blocked state to prevent the local user from requesting network services.

Examples

Place device management user **user1** in blocked state.

```
<Sysname> system-view
[Sysname] local-user user1 class manage
[Sysname-luser-manage-user1] state block
```

Related commands

display local-user

user-group

Use **user-group** to create a user group and enter its view, or enter the view of an existing user group.

Use **undo user-group** to delete a user group.

Syntax

user-group *group-name*

undo user-group *group-name*

Default

A system-defined user group exists. The group name is **system**.

Views

System view

Predefined user roles

network-admin

Parameters

group-name: Specifies the user group name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

A user group consists of a group of local users and has a set of local user attributes. You can configure local user attributes for a user group to implement centralized management of user attributes for the local users in the group.

A user group that has local users cannot be deleted.

You can modify settings for the system-defined user group named **system**, but you cannot delete the user group.

Examples

Create a user group named **abc** and enter user group view.

```
<Sysname> system-view
[Sysname] user-group abc
[Sysname-ugroup-abc]
```

Related commands

display user-group

validity-datetime

Use **validity-datetime** to specify the validity period for a network access user.

Use **undo validity-datetime** to restore the default.

Syntax

validity-datetime { **from** *start-date start-time* **to** *expiration-date expiration-time* | **from** *start-date start-time* | **to** *expiration-date expiration-time* }

undo validity-datetime

Default

The validity period for a local user does not expire.

Views

Network access user view

Predefined user roles

network-admin

Parameters

from: Specifies the validity start date and time for the user. If you do not specify this option, the command defines only the expiration date and time of the user.

start-date: Specifies the date on which the user becomes effective. The date is in the format of MM/DD/YYYY or YYYY/MM/DD. The value range for the MM argument is 1 to 12. The value range for the DD argument varies with the specified month. The value range for the YYYY argument is 2000 to 2035.

start-time: Specifies the time on the day when the user becomes effective. The time is in the format of hh:mm:ss. The value range for the hh argument is 0 to 23. The value range for the mm and ss arguments is 0 to 59. The mm and ss arguments are optional. For example, enter 1 to indicate 1:00:00. A value of 0 indicates 00:00:00.

to: Specifies the expiration date and time for the user. If you do not specify this option, the command defines only the validity start date and time of the user.

expiration-date: Specifies the expiration date in the format of MM/DD/YYYY or YYYY/MM/DD. The value range for the MM argument is 1 to 12. The value range for the DD argument varies with the specified month. The value range for the YYYY argument is 2000 to 2035.

expiration-time: Specifies the expiration time in the format of hh:mm:ss. The value range for the hh argument is 0 to 23. The value range for the mm and ss arguments is 0 to 59. The mm and ss arguments are optional. For example, enter 1 to indicate 1:00:00. A value of 0 indicates 00:00:00.

Usage guidelines

Expired network access user accounts cannot be used for authentication.

When both **from** and **to** options are specified, the expiration date and time must be later than the validity start date and time.

When only the **from** option is specified, the user is valid since the specified date and time. When only the **to** option is specified, the user is valid until the specified date and time.

Examples

Specify the validity period for network access user **123**.

```
<Sysname> system-view
[Sysname] local-user 123 class network
[Sysname-luser-network-123] validity-datetime from 2015/10/01 00:00:00 to 2016/10/02
12:00:00
```

Related commands

display local-user

RADIUS commands

aaa device-id

Use **aaa device-id** to configure the device ID.

Use **undo aaa device-id** to restore the default.

Syntax

aaa device-id *device-id*

undo aaa device-id

Default

The device ID is 0.

Views

System view

Predefined user roles

network-admin

Parameters

device-id: Specifies a device ID in the range of 1 to 255.

Usage guidelines

RADIUS uses the value of the Acct-Session-ID attribute as the accounting ID for a user. The device generates an Acct-Session-ID value for each online user based on the system time, random digits, and device ID.

If you modify the device ID, the new device ID does not take effect on users that have been online during the change.

Examples

Configure the device ID as 1.

```
<Sysname> system-view
[Sysname] aaa device-id 1
```

accounting-on enable

Use **accounting-on enable** to configure the accounting-on feature.

Use **undo accounting-on enable** to disable the accounting-on feature.

Syntax

accounting-on enable [**interval** *interval* | **send** *send-times*] *

undo accounting-on enable

Default

The accounting-on feature is disabled.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

interval *interval*: Specifies the time interval for retransmitting an accounting-on packet in seconds. The value range for the *interval* argument is 1 to 15, and the default setting is 3.

send *send-times*: Specifies the maximum number of accounting-on packet transmission attempts. The value range for the *send-times* argument is 1 to 255, and the default setting is 50.

Usage guidelines

The accounting-on feature enables the device to automatically send an accounting-on packet to the RADIUS server after a device reboot. Upon receiving the accounting-on packet, the RADIUS server logs out all online users so they can log in again through the device.

Execute the **save** command to ensure that the **accounting-on enable** command takes effect at the next device reboot. For information about the **save** command, see *Fundamentals Command Reference*.

Parameters set by using the **accounting-on enable** command take effect immediately.

Examples

Enable the accounting-on feature for RADIUS scheme **radius1**, and set the retransmission interval to 5 seconds and the transmission attempts to 15.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] accounting-on enable interval 5 send 15
```

Related commands

display radius scheme

accounting-on extended

Use **accounting-on extended** to enable the extended accounting-on feature.

Use **undo accounting-on extended** to disable the extended accounting-on feature.

Syntax

accounting-on extended

undo accounting-on extended

Default

The extended accounting-on feature is disabled.

Views

RADIUS scheme view

Predefined user roles

network-admin

network-operator

Usage guidelines

The extended accounting-on feature enhances the accounting-on feature by applying to a distributed architecture. For the extended accounting-on feature to take effect, the RADIUS server must run on IMC and the accounting-on feature must be enabled.

The extended accounting-on feature is applicable to LAN users. The user data is saved to the member devices through which the users access the IRF fabric.

When this feature is enabled, the IRF fabric automatically sends an accounting-on packet to the RADIUS server after a member device reboots (IRF fabric not reboot). The packet contains the member device identifier. Upon receiving the accounting-on packet, the RADIUS server logs out all online users that access the IRF fabric through the member device. If no users have come online through the member device, the IRF fabric does not send an accounting-on packet after the member device reboots.

The IRF fabric uses the packet retransmission interval and maximum transmission attempts set by using the **accounting-on enable** command for this feature.

Execute the **save** command to ensure that the **accounting-on extended** command takes effect at the next member device reboot. For information about the **save** command, see *Fundamentals Command Reference*.

Examples

Enable the extended accounting-on feature for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] accounting-on extended
```

Related commands

accounting-on enable

display radius scheme

attribute 5 format port

Use **attribute 5 format port** to set the NAS-Port attribute (attribute 5) format to the port format.

Use **undo attribute 5 format** to restore the default.

Syntax

attribute 5 format port

undo attribute 5 format

Default

The NAS-Port attribute uses the default format, which contains the following portions:

- 8-bit IRF member ID.
- 4-bit slot number.
- 8-bit port index.
- 12-bit VLAN ID.

Views

RADIUS scheme view

Predefined user roles

network-admin

Usage guidelines

This command is supported only in Release 6342 and later.

Perform this task to specify the format of the NAS-Port attribute (attribute 5) sent by the device to the RADIUS server. If you specify the port format, the attribute contains the value in the last segment of the user access interface. For example, if a user comes online from GigabitEthernet 1/0/2, the value for the NAS-Port attribute is 2.

To exchange RADIUS packets correctly with a RADIUS server, configure the device with the same NAS-Port attribute format as the RADIUS server.

This command takes effect on the RADIUS packets for all types of network access users.

Examples

Set the NAS-Port attribute format to the port format in RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] attribute 5 format port
```

Related commands

display radius scheme

attribute 15 check-mode

Use **attribute 15 check-mode** to configure the Login-Service attribute check method for SSH, FTP, and terminal users.

Use **undo attribute 15 check-mode** to restore the default.

Syntax

attribute 15 check-mode { **loose** | **strict** }

undo attribute 15 check-mode

Default

The strict check method applies for SSH, FTP, and terminal users.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

loose: Matches the standard Login-Service attribute value 0 for SSH, FTP, and terminal services.

strict: Matches Login-Service attribute values 50, 51, and 52 for SSH, FTP, and terminal services, respectively.

Usage guidelines

Use the loose check method only when the server does not issue Login-Service attribute values 50, 51, and 52 for SSH, FTP, and terminal users.

Examples

Configure the Login-Service attribute check method as **loose** for SSH, FTP, and terminal users in RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] attribute 15 check-mode loose
```

Related commands

display radius scheme

attribute 25 car

Use **attribute 25 car** to configure the device to interpret the RADIUS class attribute (attribute 25) as CAR parameters.

Use **undo attribute 25 car** to restore the default.

Syntax

attribute 25 car

undo attribute 25 car

Default

The RADIUS class attribute is not interpreted as CAR parameters.

Views

RADIUS scheme view

Predefined user roles

network-admin

Usage guidelines

Configure the device to interpret the RADIUS class attribute if the RADIUS server uses the attribute to deliver CAR parameters for user-based traffic monitoring and control.

Examples

In RADIUS scheme **radius1**, configure the device to interpret the RADIUS class attribute as CAR parameters.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] attribute 25 car
```

Related commands

display radius scheme

attribute 31 mac-format

Use **attribute 31 mac-format** to configure the MAC address format for RADIUS attribute 31.

Use **undo attribute 31 mac-format** to restore the default.

Syntax

attribute 31 mac-format section { **one** | { **six** | **three** } **separator** *separator-character* } { **lowercase** | **uppercase** }

undo attribute 31 mac-format

Default

A MAC address is in the format of HH-HH-HH-HH-HH-HH. The MAC address is separated by hyphens (-) into six sections with letters in upper case.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

section: Specifies the number of sections that a MAC address contains.

one: Specifies the one-section format HHHHHHHHHHHH. This keyword is available only in Release 6312 and later.

six: Specifies the six-section format HH-HH-HH-HH-HH-HH.

three: Specifies the three-section format HHHH-HHHH-HHHH.

separator *separator-character*: Specifies a case-sensitive character that separates the sections.

lowercase: Specifies the letters in a MAC address to be in lower case.

uppercase: Specifies the letters in a MAC address to be in upper case.

Usage guidelines

Configure the MAC address format for RADIUS attribute 31 to meet the requirements of the RADIUS servers.

Examples

In RADIUS scheme **radius1**, specify the MAC address format as **hh:hh:hh:hh:hh:hh** for RADIUS attribute 31.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] attribute 31 mac-format section six separator : lowercase
```

Related commands

display radius scheme

attribute 87 format interface-name

Use **attribute 87 format interface-name** to set the NAS-Port-ID attribute (attribute 87) format to the interface name format.

Use **undo attribute 87 format** to restore the default.

Syntax

attribute 87 format interface-name

undo attribute 87 format

Default

The NAS-Port-Id attribute uses the default format, which differs by user access type:

- **Default format**—The default format varies by user access type.
  - For portal users, the NAS-Port-Id attribute is in the *SlotID***00***IfNOVlanID* format:
    - *SlotID*—Represents a 2-byte IRF member ID.

        - **00**—Represents a 2-byte string of 0s.
        - *IfNO*—Represents a 3-byte port index.
        - *VLANID*—Represents a 9-byte VLAN ID.
    - For 802.1X and MAC authentication users, the NAS-Port-Id attribute is in the **slot=***xx***;subslot=***xx***;port=***xx***;vlanid=***xx* format.
        - **slot**—IRF member ID.
        - **subslot**—Slot number.
        - **port**—Port index.
        - **vlanid**—VLAN ID
- For login users, the device does not include the NAS-Port-Id attribute in RADIUS packets.

Views

RADIUS scheme view

Predefined user roles

network-admin

Usage guidelines

This command is supported only in Release 6342 and later.

Perform this task to specify the format of the NAS-Port-ID attribute (attribute 87) sent by the device to the RADIUS server. If you specify the interface name format, the attribute contains the name of the user access interface. For example, if a user access the network from GigabitEthernet 1/0/1, the NAS-Port-ID attribute is set to **GigabitEthernet1/0/1**.

To exchange RADIUS packets correctly with a RADIUS server, configure the device with the same NAS-Port-ID attribute format as the RADIUS server.

This command takes effect on the RADIUS packets for all types of network access users.

Examples

Set the NAS-Port-ID attribute format to the interface name format in RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] attribute 87 format interface-name
```

Related commands

display radius scheme

attribute convert (RADIUS DAS view)

Use **attribute convert** to configure a RADIUS attribute conversion rule.

Use **undo attribute convert** to delete RADIUS attribute conversion rules.

Syntax

attribute convert *src-attr-name* **to** *dest-attr-name* { { **coa-ack** | **coa-request** } * | { **received** | **sent** } * }

undo attribute convert [*src-attr-name*]

Default

No RADIUS attribute conversion rules exist. The system processes RADIUS attributes according to the principles of the standard RADIUS protocol.

Views

RADIUS DAS view

Predefined user roles

network-admin

Parameters

src-attr-name: Specifies the source RADIUS attribute by its name, a case-insensitive string of 1 to 63 characters. The attribute must be supported by the system.

dest-attr-name: Specifies the destination RADIUS attribute by its name, a case-insensitive string of 1 to 63 characters. The attribute must be supported by the system.

coa-ack: Specifies the CoA acknowledgment packets.

coa-request: Specifies the CoA request packets.

received: Specifies the received DAE packets.

sent: Specifies the sent DAE packets.

Usage guidelines

The device replaces the attribute in packets that match a RADIUS attribute conversion rule with the destination RADIUS attribute in the rule.

The conversion rules take effect only when the RADIUS attribute translation feature is enabled.

When you configure RADIUS attribute conversion rules, follow these restrictions and guidelines:

- The source and destination RADIUS attributes in a rule must use the same data type.
- The source and destination RADIUS attributes in a rule cannot use the same name.
- A source RADIUS attribute can be converted only by one criterion, packet type or direction.
- One source RADIUS attribute cannot be converted to multiple destination attributes.

If you do not specify a source RADIUS attribute, the **undo attribute convert** command deletes all RADIUS attribute conversion rules.

Examples

In RADIUS DAS view, configure a RADIUS attribute conversion rule to replace the Hw-Server-String attribute in the received DAE packets with the Connect-Info attribute.

```
<Sysname> system-view
[Sysname] radius dynamic-author server
[Sysname-radius-da-server] attribute convert Hw-Server-String to Connect-Info received
```

Related commands

attribute translate

attribute convert (RADIUS scheme view)

Use **attribute convert** to configure a RADIUS attribute conversion rule.

Use **undo attribute convert** to delete RADIUS attribute conversion rules.

Syntax

attribute convert *src-attr-name* **to** *dest-attr-name* { { **access-accept** | **access-request** | **accounting** } * | { **received** | **sent** } * }

undo attribute convert [*src-attr-name*]

Default

No RADIUS attribute conversion rules exist. The system processes RADIUS attributes according to the principles of the standard RADIUS protocol.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

src-attr-name: Specifies the source RADIUS attribute by its name, a case-insensitive string of 1 to 63 characters. The attribute must be supported by the system.

dest-attr-name: Specifies the destination RADIUS attribute by its name, a case-insensitive string of 1 to 63 characters. The attribute must be supported by the system.

access-accept: Specifies the RADIUS Access-Accept packets.

access-request: Specifies the RADIUS Access-Request packets.

accounting: Specifies the RADIUS accounting packets.

received: Specifies the received RADIUS packets.

sent: Specifies the sent RADIUS packets.

Usage guidelines

The device replaces the attribute in packets that match a RADIUS attribute conversion rule with the destination RADIUS attribute in the rule.

The conversion rules take effect only when the RADIUS attribute translation feature is enabled.

When you configure RADIUS attribute conversion rules, follow these restrictions and guidelines:

- The source and destination RADIUS attributes in a rule must use the same data type.
- The source and destination RADIUS attributes in a rule cannot use the same name.
- A source RADIUS attribute can be converted only by one criterion, packet type or direction.
- One source RADIUS attribute cannot be converted to multiple destination attributes.

If you do not specify a source RADIUS attribute, the **undo attribute convert** command deletes all RADIUS attribute conversion rules.

Examples

In RADIUS scheme **radius1**, configure a RADIUS attribute conversion rule to replace the Hw-Server-String attribute of received RADIUS packets with the Connect-Info attribute.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] attribute convert Hw-Server-String to Connect-Info received
```

Related commands

attribute translate

attribute reject (RADIUS DAS view)

Use **attribute reject** to configure a RADIUS attribute rejection rule.

Use **undo attribute reject** to delete RADIUS attribute rejection rules.

Syntax

attribute reject *attr-name* { { **coa-ack** | **coa-request** } * | { **received** | **sent** } * }

undo attribute reject [*attr-name*]

Default

No RADIUS attribute rejection rules exist.

Views

RADIUS DAS view

Predefined user roles

network-admin

Parameters

attr-name: Specifies a RADIUS attribute by its name, a case-insensitive string of 1 to 63 characters. The attribute must be supported by the system.

coa-ack: Specifies the CoA acknowledgment packets.

coa-request: Specifies the CoA request packets.

received: Specifies the received DAE packets.

sent: Specifies the sent DAE packets.

Usage guidelines

Configure RADIUS attribute rejection rules for the following purposes:

- Delete attributes from the RADIUS packets to be sent if the destination RADIUS server does not identify the attributes.
- Ignore unwanted attributes in the RADIUS packets received from a RADIUS server.

The RADIUS attribute rejection rules take effect only when the RADIUS attribute translation feature is enabled.

A RADIUS attribute can be rejected only by one criterion, packet type or direction.

If you do not specify a RADIUS attribute, the **undo attribute reject** command deletes all RADIUS attribute rejection rules.

Examples

In RADIUS DAS view, configure a RADIUS attribute rejection rule to delete the Connect-Info attribute from the DAE packets to be sent.

```
<Sysname> system-view
[Sysname] radius dynamic-author server
[Sysname-radius-da-server] attribute reject Connect-Info sent
```

Related commands

attribute translate

attribute reject (RADIUS scheme view)

Use **attribute reject** to configure a RADIUS attribute rejection rule.

Use **undo attribute reject** to delete RADIUS attribute rejection rules.

Syntax

attribute reject *attr-name* { { **access-accept** | **access-request** | **accounting** } * | { **received** | **sent** } * }

undo attribute reject [*attr-name*]

Default

No RADIUS attribute rejection rules exist.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

attr-name: Specifies a RADIUS attribute by its name, a case-insensitive string of 1 to 63 characters. The attribute must be supported by the system.

access-accept: Specifies the RADIUS Access-Accept packets.

access-request: Specifies the RADIUS Access-Request packets.

accounting: Specifies the RADIUS accounting packets.

received: Specifies the received RADIUS packets.

sent: Specifies the sent RADIUS packets.

Usage guidelines

Configure RADIUS attribute rejection rules for the following purposes:

- Delete attributes from the RADIUS packets to be sent if the destination RADIUS server does not identify the attributes.
- Ignore unwanted attributes in the RADIUS packets received from a RADIUS server.

The RADIUS attribute rejection rules take effect only when the RADIUS attribute translation feature is enabled.

A RADIUS attribute can be rejected only by one criterion, packet type or direction.

If you do not specify a RADIUS attribute, the **undo attribute reject** command deletes all RADIUS attribute rejection rules.

Examples

In RADIUS scheme **radius1**, configure a RADIUS attribute rejection rule to delete the Connect-Info attribute from the RADIUS packets to be sent.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] attribute reject Connect-Info sent
```

Related commands

attribute translate

attribute remanent-volume

Use **attribute remanent-volume** to set the data measurement unit for the Remanent_Volume attribute.

Use **undo attribute remanent-volume** to restore the default.

Syntax

attribute remanent-volume unit { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** }

undo attribute remanent-volume unit

Default

The data measurement unit is kilobyte for the Remanent_Volume attribute.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

byte: Specifies the unit as byte.

giga-byte: Specifies the unit as gigabyte.

kilo-byte: Specifies the unit as kilobyte.

mega-byte: Specifies the unit as megabyte.

Usage guidelines

Make sure the measurement unit is the same as the user data measurement unit on the RADIUS server.

Examples

In RADIUS scheme **radius1**, set the data measurement unit to **kilobyte** for the Remanent_Volume attribute.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] attribute remanent-volume unit kilo-byte
```

Related commands

display radius scheme

attribute translate

Use **attribute translate** to enable the RADIUS attribute translation feature.

Use **undo attribute translate** to disable the RADIUS attribute translation feature.

Syntax

attribute translate

undo attribute translate

Default

The RADIUS attribute translation feature is disabled.

Views

RADIUS DAS view

RADIUS scheme view

Predefined user roles

network-admin

Usage guidelines

To cooperate with RADIUS servers of different vendors, enable the RADIUS attribute translation feature. Configure RADIUS attribute conversion rules and rejection rules to ensure that RADIUS attributes in the packets exchanged between the device and the server are supported by both sides.

Examples

Enable the RADIUS attribute translation feature for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] attribute translate
```

Related commands

attribute convert (RADIUS DAS view)

attribute convert (RADIUS scheme view)

attribute reject (RADIUS DAS view)

attribute reject (RADIUS scheme view)

ca-file

Use **ca-file** to specify a CA certificate file for EAP authentication.

Use **undo ca-file** to restore the default.

Syntax

ca-file *file-name*

undo ca-file

Default

No CA certificate file is specified for EAP authentication. The device does not verify the RADIUS server certificate during EAP authentication.

Views

EAP profile view

Predefined user roles

network-admin

Parameters

file-name: Specifies a CA certificate file by its name, a case-sensitive string of 1 to 91 characters.

Usage guidelines

You must specify a CA certificate file to verify the RADIUS server certificate if the EAP authentication method is PEAP-GTC, PEAP-MSCHAPv2, TTLS-GTC, or TTLS-MSCHAPv2.

Before you specify a CA certificate file, you must use FTP or TFTP to transfer the CA certificate file to the root directory of the default storage medium on the device.

In an IRF fabric, make sure a CA certificate file already exists in the root directory of the default storage medium on the master device before you specify the file.

You can specify only one CA certificate file in an EAP profile. If you execute this command multiple times, the most recent configuration takes effect.

If you change the CA certificate file, the new CA certificate file takes effect at the next server status detection.

Examples

In EAP profile **eap1**, specify CA certificate file **CA.der** for EAP authentication.

```
<Sysname> system-view
[Sysname] eap-profile eap1
[Sysname-eap-profile-eap1] ca-file CA.der
```

client

Use **client** to specify a RADIUS DAC.

Use **undo client** to remove a RADIUS DAC.

Syntax

client { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**key** { **cipher** | **simple** } *string*]

undo client { **ip** *ipv4-address* | **ipv6** *ipv6-address* }

Default

No RADIUS DACs are specified.

Views

RADIUS DAS view

Predefined user roles

network-admin

Parameters

ip *ipv4-address*: Specifies a DAC by its IPv4 address.

ipv6 *ipv6-address*: Specifies a DAC by its IPv6 address.

key: Specifies the shared key for secure communication between the RADIUS DAC and server. Make sure the shared key is the same as the key configured on the RADIUS DAC. If the RADIUS DAC does not have any shared key, do not specify this option.

cipher: Specifies the key in encrypted form.

simple: Specifies the key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive. In non-FIPS mode, the encrypted form of the key is a string of 1 to 117 characters. The plaintext form of the key is a string of 1 to 64 characters. In FIPS mode, the encrypted form of the key is a string of 15 to 117 characters. The plaintext form of the key is a string of 15 to 64 characters. The plaintext string must contain characters from digits, uppercase letters, lowercase letters, and special characters.

Usage guidelines

With the RADIUS DAS feature, the device listens to the default or specified UDP port to receive DAE requests from the specified DACs. The device processes the requests and sends DAE responses to the DACs.

The device discards any DAE packets sent from DACs that are not specified for the DAS.

You can execute the **client** command multiple times to specify multiple DACs for the DAS.

Examples

Specify the DAC as 10.110.1.2. Set the shared key to **123456** in plaintext form for secure communication between the DAS and DAC.

```
<Sysname> system-view
[Sysname] radius dynamic-author server
[Sysname-radius-da-server] client ip 10.110.1.2 key simple 123456
```

Related commands

radius dynamic-author server

port

data-flow-format (RADIUS scheme view)

Use **data-flow-format** to set the data flow and packet measurement units for traffic statistics.

Use **undo data-flow-format** to restore the default.

Syntax

data-flow-format { **data** { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** } | **packet** { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** } } *

undo data-flow-format { **data** | **packet** }

Default

Traffic is counted in bytes and packets.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

data: Specifies the unit for data flows.

byte: Specifies the unit as byte.

giga-byte: Specifies the unit as gigabyte.

kilo-byte: Specifies the unit as kilobyte.

mega-byte: Specifies the unit as megabyte.

packet: Specifies the unit for data packets.

giga-packet: Specifies the unit as giga-packet.

kilo-packet: Specifies the unit as kilo-packet.

mega-packet: Specifies the unit as mega-packet.

one-packet: Specifies the unit as one-packet.

Usage guidelines

The data flow and packet measurement units for traffic statistics must be the same as configured on the RADIUS accounting servers. Otherwise, accounting results might be incorrect.

Examples

In RADIUS scheme **radius1**, set the data flow and packet measurement units for traffic statistics to kilobyte and kilo-packet, respectively.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] data-flow-format data kilo-byte packet kilo-packet
```

Related commands

display radius scheme

display radius scheme

Use **display radius scheme** to display RADIUS scheme configuration.

Syntax

display radius scheme [*radius-scheme-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

radius-scheme-name: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters. If you do not specify a RADIUS scheme, this command displays the configuration of all RADIUS schemes.

Examples

Display the configuration of all RADIUS schemes.

```
<Sysname> display radius scheme
Total 1 RADIUS schemes

----------------------------------------------------------------------
RADIUS scheme name: radius1
  Index : 0
  Primary authentication server:
    Host name: Not configured
    IP   : 2.2.2.2                                Port: 1812
    VPN  : Not configured
    State: Active
    Test profile: 132
      Probe username: test
      Probe interval: 60 minutes
      Probe eap-profile: eap1
    Weight: 40
  Primary accounting server:
    Host name: Not configured
    IP   : 1.1.1.1                                Port: 1813
    VPN  : Not configured
    State: Active
    Weight: 40
  Second authentication server:
    Host name: Not configured
    IP   : 3.3.3.3                                Port: 1812
    VPN  : Not configured
```

```
    State: Block
    Test profile: Not configured
    Weight: 40
  Second accounting server:
    Host name: Not configured
    IP   : 3.3.3.3                                  Port: 1813
    VPN  : Not configured
    State: Block (Mandatory)
    Weight: 0
  Accounting-On function                     : Enabled
    extended function                        : Disabled
    retransmission times                     : 5
    retransmission interval(seconds)         : 2
  Timeout Interval(seconds)                  : 3
  Retransmission Times                       : 3
  Retransmission Times for Accounting Update : 5
  Server Quiet Period(minutes)               : 5
  Realtime Accounting Interval(seconds)      : 22
  Stop-accounting packets buffering          : Enabled
    Retransmission times                     : 500
  NAS IP Address                             : 1.1.1.1
  VPN                                        : Not configured
  User Name Format                           : with-domain
  Data flow unit                             : Megabyte
  Packet unit                                : One
  Attribute 5 format                         : Port
  Attribute 15 check-mode                    : Strict
  Attribute 25                               : CAR
  Attribute 87 format                        : Interface name
  Attribute Remanent-Volume unit             : Mega
  server-load-sharing                        : Enabled
  Attribute 31 MAC format                    : hh:hh:hh:hh:hh:hh
  Stop-accounting-packet send-force          : Disabled
  Reauthentication server selection          : Reselect
------------------------------------------------------------------------
```

Table 4 Command output

Field	Description
Index	Index number of the RADIUS scheme.
Primary authentication server	Information about the primary authentication server.
Primary accounting server	Information about the primary accounting server.
Second authentication server	Information about the secondary authentication server.
Second accounting server	Information about the secondary accounting server.
Host name	Host name of the server. This field displays **Not configured** in the following situations: • The server is not configured. • The server is specified by IP address.

Field	Description
IP	IP address of the server. This field displays **Not configured** in the following situations: • The server is not configured. • The server is specified by hostname, and the hostname is not resolved.
Port	Service port number of the server. If no port number is specified, this field displays the default port number.
VPN	This field is not supported in the current software version. MPLS L3VPN instance to which the server or the RADIUS scheme belongs. If no VPN instance is specified for the server, this field displays **Not configured**.
State	Status of the server: • **Active**—The server is in active state. • **Block**—The server is changed to blocked state automatically. • **Block (Mandatory)**—The server is set to blocked state manually.
Test profile	Test profile used for RADIUS server status detection.
Probe username	Username used for RADIUS server status detection.
Probe interval	Server status detection interval, in minutes.
Probe eap-profile	EAP profile specified for RADIUS server status detection. This field is not available if no EAP profile is specified in the test profile for RADIUS server status detection.
Weight	Weight value of the RADIUS server.
Accounting-On function	Whether the accounting-on feature is enabled.
extended function	Whether the extended accounting-on feature is enabled.
retransmission times	Number of accounting-on packet transmission attempts.
retransmission interval(seconds)	Interval at which the device retransmits accounting-on packets, in seconds.
Timeout Interval(seconds)	RADIUS server response timeout period, in seconds.
Retransmission times	Maximum number of attempts for transmitting a RADIUS packet to a single RADIUS server.
Retransmission Times for Accounting Update	Maximum number of accounting attempts.
Server Quiet Period(minutes)	Quiet period for the servers, in minutes.
Realtime Accounting Interval(seconds)	Interval for sending real-time accounting updates, in seconds.
Stop-accounting packets buffering	Whether buffering of nonresponded RADIUS stop-accounting requests is enabled.
Retransmission times	Maximum number of transmission attempts for individual RADIUS stop-accounting requests.
NAS IP Address	Source interface or source IP addresses for outgoing RADIUS packets. This field displays **Not configured** if no source interface or source IP addresses are specified for outgoing RADIUS packets.
User Name Format	Format for the usernames sent to the RADIUS server: • **with-domain**—Includes the domain name.

Field	Description
	• **without-domain**—Excludes the domain name. • **keep-original**—Forwards the username as the username is entered.
Data flow unit	Measurement unit for data flow.
Packet unit	Measurement unit for packets.
Attribute 5 format	This field is supported only in Release 6342 and later. NAS-Port attribute (attribute 5) format options: • **Port**. • **Default**.
Attribute 15 check-mode	RADIUS Login-Service attribute check method for SSH, FTP, and terminal users: • **Strict**—Matches Login-Service attribute values 50, 51, and 52 for SSH, FTP, and terminal services, respectively. • **Loose**—Matches the standard Login-Service attribute value 0 for SSH, FTP, and terminal services.
Attribute 25	RADIUS attribute 25 interpretation status: • **Standard**—The attribute is not interpreted as CAR parameters. • **CAR**—The attribute is interpreted as CAR parameters.
Attribute 87 format	This field is supported only in Release 6342 and later. NAS-Port-ID attribute (attribute 87) format options: • **Interface name**. • **Default**.
Attribute Remanent-Volume unit	Data measurement unit for the RADIUS Remanent_Volume attribute.
server-load-sharing	Status of the RADIUS server load sharing feature: • **Disabled**—The feature is disabled. The device forwards traffic to the server selected based on primary and secondary server roles. • **Enabled**—The feature is enabled. The device distributes traffic among multiple servers for load sharing.
Attribute 31 MAC format	MAC address format for RADIUS attribute 31.
Stop-accounting-packet send-force	Whether the device is enabled to forcibly send stop-accounting packets when users for which no start-accounting packets are sent go offline.
Reauthentication server selection	This field is not supported in the current software version. RADIUS server selection mode in reauthentication: • **Inherit**—The device uses the RADIUS server that performed authentication for a user to reauthenticate that user. • **Reselect**—The device searches for a reachable RADIUS server to reauthenticate a user.

display radius server-load statistics

Use **display radius server-load statistics** to display authentication and accounting load statistics for all RADIUS servers.

Syntax

display radius server-load statistics

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

This command displays the following statistics:

- **Last-5-second statistics**—Total number of authentication or accounting requests sent to each RADIUS server in the last 5 seconds.
- **History statistics**—Total number of authentication or accounting requests sent to each RADIUS server since the device starts up.

The device collects the statistics as follows:

- **Last-5-second statistics**—From the device sends the first authentication or accounting request to a RADIUS server, the device counts the number of authentication or accounting requests sent to the server every 5 seconds. Then, the device updates the last-5-second authentication and accounting statistics for the server.
- **History statistics**—The device increases the history statistics for a RADIUS server by 1 each time it sends an authentication or accounting request to the server. The device does not decrease the history statistics even though users go offline or the server fails to response to a request within the timeout time.

Based on the statistics, you can adjust the load on RADIUS servers by changing the sequence in which the servers are configured or the weight values of the servers.

This command displays statistics only for RADIUS servers whose IP addresses are available or can be resolved from their hostnames.

The device deletes all statistics for a RADIUS server if the server is removed from a RADIUS scheme or the server's IP address or service port number changes.

If an active/standby switchover occurs, the last-5-second statistics are deleted. However, the history statistics are not deleted. The history statistics might be inaccurate.

If the device reboots, both the last-5-seconds statistics and the history statistics are deleted.

Examples

Display authentication and accounting load statistics for all RADIUS servers.

```
<Sysname> display radius server-load statistics
Authentication servers: 2
IP                   VPN              Port    Last 5 sec   History
1.1.1.1              N/A              1812    20           100
2.2.2.2              N/A              1812    0            20
Accounting servers: 2
IP                   VPN              Port    Last 5 sec   History
1.1.1.1              N/A              1813    20           100
2.2.2.2             N/A              1813    0            20
```

Table 5 Command output

Field	Description
Authentication servers	Total number of RADIUS authentication servers.
Accounting servers	Total number of RADIUS accounting servers.

Field	Description
IP	IP address of a RADIUS server.
VPN	This field is not supported in the current software version. MPLS L3VPN instance to which the RADIUS server belongs. This field displays **N/A** if no VPN instance is specified for the server.
Port	Service port number of the RADIUS server.
Last 5 sec	Total number of RADIUS authentication or accounting requests sent to the RADIUS server within the last 5 seconds.
History	Total number of RADIUS authentication or accounting requests sent to the RADIUS server since the device starts up.

Related commands

`reset radius server-load statistics`

display radius statistics

Use **`display radius statistics`** to display RADIUS packet statistics.

Syntax

`display radius statistics`

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display RADIUS packet statistics.

```
<Sysname> display radius statistics

                            Auth.         Acct.       SessCtrl.
          Request Packet:     0             0             0
            Retry Packet:     0             0             -
          Timeout Packet:     0             0             -
       Access Challenge:      0             -             -
           Account Start:     -             0             -
          Account Update:     -             0             -
            Account Stop:     -             0             -
      Terminate Request:      -             -             0
             Set Policy:      -             -             0
   Packet With Response:      0             0             0
Packet Without Response:      0             0             -
          Access Rejects:     0             -             -
          Dropped Packet:     0             0             0
          Check Failures:     0             0             0
```

Table 6 Command output

Field	Description
Auth.	Authentication packets.
Acct.	Accounting packets.
SessCtrl.	Session-control packets.
Request Packet	Number of request packets.
Retry Packet	Number of retransmitted request packets.
Timeout Packet	Number of request packets timed out.
Access Challenge	Number of access challenge packets.
Account Start	Number of start-accounting packets.
Account Update	Number of accounting update packets.
Account Stop	Number of stop-accounting packets.
Terminate Request	Number of packets for logging off users forcibly.
Set Policy	Number of packets for updating user authorization information.
Packet With Response	Number of packets for which responses were received.
Packet Without Response	Number of packets for which no responses were received.
Access Rejects	Number of Access-Reject packets.
Dropped Packet	Number of discarded packets.
Check Failures	Number of packets with checksum errors.

Related commands

`reset radius statistics`

display stop-accounting-buffer (for RADIUS)

Use **`display stop-accounting-buffer`** to display information about buffered RADIUS stop-accounting requests to which no responses have been received.

Syntax

`display stop-accounting-buffer` { **`radius-scheme`** *`radius-scheme-name`* | **`session-id`** *`session-id`* | **`time-range`** *`start-time end-time`* | **`user-name`** *`user-name`* }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

`radius-scheme` *`radius-scheme-name`*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

session-id *session-id*: Specifies a session by its ID. The *session-id* argument is a string of 1 to 64 characters and cannot contain a letter. A session ID uniquely identifies an online user for a RADIUS scheme.

time-range *start-time end-time*: Specifies a time range. The start time and end time must be in the format of hh:mm:ss-mm/dd/yyyy or hh:mm:ss-yyyy/mm/dd.

user-name *user-name*: Specifies a user by its name, a case-sensitive string of 1 to 255 characters. Whether the *user-name* argument should include the domain name depends on the setting configured by using the **user-name-format** command for the RADIUS scheme.

Examples

Display information about nonresponded RADIUS stop-accounting requests buffered for user **abc**.

```
<Sysname> display stop-accounting-buffer user-name abc
Total entries: 2
Scheme     Session ID          Username    First sending time   Attempts
rad1       1000326232325010    abc         23:27:16-08/31/2015  19
aaa        1000326232326010    abc         23:33:01-08/31/2015  20
```

Table 7 Command output

Field	Description
Session ID	Session ID, which is the value of attribute Acct-Session-Id.
First sending time	Time when the stop-accounting request was first sent.
Attempts	Number of attempts that were made to send the stop-accounting request.

Related commands

reset stop-accounting-buffer (for RADIUS)

retry

retry stop-accounting (RADIUS scheme view)

stop-accounting-buffer enable (RADIUS scheme view)

user-name-format (RADIUS scheme view)

eap-profile

Use **eap-profile** to create an EAP profile and enter its view, or enter the view of an existing EAP profile.

Use **undo eap-profile** to delete an EAP profile.

Syntax

eap-profile *eap-profile-name*

undo eap-profile *eap-profile-name*

Default

No EAP profiles exist.

Views

System view

Predefined user roles

network-admin

Parameters

eap-profile-name: Specifies the EAP profile name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

An EAP profile is a collection of EAP authentication settings, including the EAP authentication method and the CA certificate file to be used for some EAP authentication methods. You can use an EAP profile in a test profile for RADIUS server status detection.

You can specify an EAP profile in multiple test profiles.

You can configure a maximum of 16 EAP profiles.

Examples

Create an EAP profile named **eap1** and enter its view.

```
<Sysname> system-view
[Sysname] eap-profile eap1
[Sysname-eap-profile-eap1]
```

Related commands

radius-server test-profile

exclude

Use **exclude** to exclude an attribute from RADIUS requests.

Use **undo exclude** to cancel the configuration of excluding an attribute from RADIUS requests.

Syntax

exclude { **accounting** | **authentication** } **name** *attribute-name*

undo exclude { **accounting** | **authentication** } **name** *attribute-name*

Default

No attributes are configured to be excluded from RADIUS requests.

Views

RADIUS attribute test group view

Predefined user roles

network-admin

Parameters

accounting: Specifies RADIUS accounting requests.

authentication: Specifies RADIUS authentication requests.

name *attribute-name*: Specifies a RADIUS attribute by its name, a case-insensitive string of 1 to 63 characters. The specified attribute must be an attribute that RADIUS requests carry by default. RADIUS authentication requests carry the following attributes by default: Service-Type, Framed-Protocol, NAS-Identifier, Acct-Session-Id, and NAS-Port-Type. RADIUS accounting requests carry the following attributes by default: NAS-Identifier, Acct-Delay-Time, Acct-Session-Id, and Acct-Terminate-Cause.

Usage guidelines

Use this command to exclude an attribute from RADIUS requests sent during an AAA test to help troubleshoot authentication or accounting failures.

Before you exclude an attribute that is already configured to be included in RADIUS requests, you must cancel the inclusion configuration by using the **undo include** command.

Examples

In RADIUS attribute test group **t1**, exclude Service-Type attribute from RADIUS authentication requests.

```
<Sysname> system-view
[Sysname] radius attribute-test-group t1
[Sysname-radius-attr-test-grp-t1] exclude authentication name Service-Type
```

Related commands

include

test-aaa

include

Use **include** to include an attribute in RADIUS requests.

Use **undo include** to cancel the configuration of including an attribute in RADIUS requests.

Syntax

include { **accounting** | **authentication** } { **name** *attribute-name* | [**vendor** *vendor-id*] **code** *attribute-code* } **type** { **binary** | **date** | **integer** | **interface-id** | **ip** | **ipv6** | **ipv6-prefix** | **octets** | **string** } **value** *attribute-value*

undo include { **accounting** | **authentication**} { **name** *attribute-name* | [**vendor** *vendor-id*] **code** *attribute-code* }

Default

No attributes are configured to be included in RADIUS authentication or accounting requests.

Views

RADIUS attribute test group view

Predefined user roles

network-admin

Parameters

accounting: Specifies RADIUS accounting requests.

authentication: Specifies RADIUS authentication requests.

name *attribute-name*: Specifies a standard RADIUS attribute by its name, a case-insensitive string of 1 to 63 characters.

vendor *vendor-id*: Specifies a vendor by its ID in the range of 1 to 65535. If the attribute is a standard RADIUS attribute, do not specify this option.

code *attribute-code*: Specifies a RADIUS attribute by its code in the range of 1 to 255.

type: Specifies a data type for the attribute content.

binary: Binary type.

date: Date type.

integer: Integer type.

interface-id: Interface ID type.

ip: IPv4 address type.

ipv6: IPv6 address type.

ipv6-prefix: IPv6 address prefix type.

octets: Octet type.

string: String type.

value *attribute-value*: Specifies the value for the attribute of the data type. The value range of the *attribute-value* argument varies by data type.

- For the binary type, the value is a string of 1 to 256 hexadecimal characters, which represents a binary number with a maximum of 128 bytes.
- For the date type, the value range is 0 to 4294967295.
- For the integer type, the value range is 0 to 4294967295.
- For the interface ID type, the value range is 1 to ffffffffffffffff.
- For the IPv6 address prefix type, the value is in the format of *prefix*/*prefix-length*.
- For the octet type, the value is a string of 1 to 256 hexadecimal characters, which represents an octet number with a maximum of 128 bytes.
- For the string type, the value of this argument is a string of 1 to 253 characters.

Usage guidelines

Use this command to add an attribute that RADIUS requests do not carry by default to the RADIUS requests. The **undo** form of this command removes the attribute from the RADIUS requests.

For an attribute that RADIUS requests carry by default, you can use this command to change its value. The **undo** form of this command restores the attribute value to the default.

Table 8 shows the attributes that RADIUS requests carry by default.

Table 8 Attributes that RADIUS requests carry by default

Packet type	Attributes that the type of packets carry by default
RADIUS authentication request	User-Name, CHAP-Password (or User-Password), CHAP-Challenge, NAS-IP-Address (or NAS-IPv6-Address), Service-Type,Framed-Protocol, NAS-Identifier, NAS-Port-Type, and Acct-Session-Id.
RADIUS accounting request	User-Name, Acct-Status-Type, NAS-IP-Address (or NAS-IPv6-Address), NAS-Identifier, Acct-Session-Id, Acct-Delay-Time, and Acct-Terminate-Cause.

For the accuracy of AAA tests, the value of an attribute must be of the data type specified for that attribute.

The attribute names of standard attributes saved in the configuration file will be converted to attribute codes.

Before you include an attribute that is already configured to be excluded from RADIUS requests, you must cancel the exclusion configuration by using the **undo exclude** command.

Plan the RADIUS attributes to be included in RADIUS requests. Besides the attributes carried by default, the device adds the specified attributes to RADIUS packets in the order that they are

specified by using the **include** command. Additional attributes cannot be added to a RADIUS request if the length of the RADIUS request reaches 4096 bytes.

Examples

In RADIUS attribute test group **t1**, include Calling-Station-Id attribute with value 08-00-27-00-34-D8 in RADIUS authentication requests.

```
<Sysname> system-view
[Sysname] radius attribute-test-group t1
[Sysname-radius-attr-test-grp-t1] include authentication name Calling-Station-Id type string value 08-00-27-00-34-d8
```

Related commands

exclude

test-aaa

key (RADIUS scheme view)

Use **key** to set the shared key for secure RADIUS authentication or accounting communication.

Use **undo key** to delete the shared key for secure RADIUS authentication or accounting communication.

Syntax

key { **accounting** | **authentication** } { **cipher** | **simple** } *string*

undo key { **accounting** | **authentication** }

Default

No shared key is configured for secure RADIUS authentication or accounting communication.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

accounting: Specifies the shared key for secure RADIUS accounting communication.

authentication: Specifies the shared key for secure RADIUS authentication communication.

cipher: Specifies the key in encrypted form.

simple: Specifies the key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive. In non-FIPS mode, the encrypted form of the key is a string of 1 to 117 characters. The plaintext form of the key is a string of 1 to 64 characters. In FIPS mode, the encrypted form of the key is a string of 15 to 117 characters. The plaintext form of the key is a string of 15 to 64 characters. The plaintext string must contain digits, uppercase letters, lowercase letters, and special characters.

Usage guidelines

The shared keys configured by using this command apply to all servers in the scheme. Make sure the settings match the shared keys configured on the RADIUS servers.

The shared keys specified for specific RADIUS servers take precedence over the shared key specified with this command.

Examples

In RADIUS scheme **radius1**, set the shared key to **ok** in plaintext form for secure accounting communication.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] key accounting simple ok
```

Related commands

display radius scheme

method

Use **method** to specify the EAP authentication method.

Use **undo method** to restore the default.

Syntax

method { **md5** | **peap-gtc** | **peap-mschapv2** | **ttls-gtc** | **ttls-mschapv2** }

undo method

Default

MD5-challenge authentication is used.

Views

EAP profile view

Predefined user roles

network-admin

Parameters

md5: Specifies the MD5-challenge method.

peap-gtc: Specifies the PEAP-GTC method.

peap-mschapv2: Specifies the PEAP-MSCHAPv2 method.

ttls-gtc: Specifies the TTLS-GTC method.

ttls-mschapv2: Specifies the TTLS-MSCHAPv2 method.

Usage guidelines

You must specify an EAP authentication method that is supported by the RADIUS server to be detected.

You can specify only one EAP authentication method in an EAP profile. If you execute this command multiple times, the most recent configuration takes effect.

If you change the EAP authentication method, the new method takes effect in the next server status detection.

Examples

In EAP profile **eap1**, specify PEAP-GTC as the EAP authentication method.

```
<Sysname> system-view
[Sysname] eap-profile eap1
[Sysname-eap-profile-eap1] method peap-gtc
```

nas-ip (RADIUS scheme view)

Use **nas-ip** to specify a source interface or source IP address for outgoing RADIUS packets.

Use **undo nas-ip** to delete the specified source interface or source IP address for outgoing RADIUS packets.

Syntax

nas-ip { *ipv4-address* | **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }

undo nas-ip [**interface** | **ipv6**]

Default

The source IP address of an outgoing RADIUS packet is that specified by using the **radius nas-ip** command in system view.

If the **radius nas-ip** command is not used, the source IP address is the primary IP address of the outbound interface.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a source interface by its type and number. The device uses the primary IPv4 address or the IPv6 address of the interface as the source IP address of an outgoing RADIUS packet.

ipv4-address: Specifies an IPv4 address, which must be an address of the device. The IP address cannot be 0.0.0.0, 255.255.255.255, a class D address, a class E address, or a loopback address.

ipv6 *ipv6-address*: Specifies an IPv6 address, which must be a unicast address of the device and cannot be a loopback address or a link-local address.

Usage guidelines

The source IP address of RADIUS packets that a NAS sends must match the IP address of the NAS that is configured on the RADIUS server. A RADIUS server identifies a NAS by its IP address. Upon receiving a RADIUS packet, the RADIUS server checks the source IP address of the packet.

- If the source IP address of the packet is the IP address of a managed NAS, the server processes the packet.
- If the source IP address of the packet is not the IP address of a managed NAS, the server drops the packet.

As a best practice, specify a loopback interface address as the source IP address for outgoing RADIUS packets to avoid RADIUS packet loss caused by physical port errors.

If you use both the **nas-ip** command and **radius nas-ip** command, the following guidelines apply:

- The setting configured by using the **nas-ip** command in RADIUS scheme view applies only to the RADIUS scheme.
- The setting configured by using the **radius nas-ip** command in system view applies to all RADIUS schemes.
- The setting in RADIUS scheme view takes precedence over the setting in system view.

For a RADIUS scheme, the following restrictions apply:

- You can specify only one source IPv4 address and one source IPv6 address for outgoing RADIUS packets.
- You can specify only one source interface to provide the source IP address for outgoing RADIUS packets. Make sure the route between the source interface and the RADIUS server is reachable.
- The source interface configuration and the source IP address configuration overwrite each other.

If you do not specify any parameter for the **undo nas-ip** command, the command deletes the specified source IPv4 address for outgoing RADIUS packets.

Examples

In RADIUS scheme **radius1**, specify IP address 10.1.1.1 as the source IP address for outgoing RADIUS packets.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] nas-ip 10.1.1.1
```

Related commands

display radius scheme

radius nas-ip

port

Use **port** to specify the RADIUS DAS port.

Use **undo port** to restore the default.

Syntax

port *port-number*

undo port

Default

The RADIUS DAS port number is 3799.

Views

RADIUS DAS view

Predefined user roles

network-admin

Parameters

port-number: Specifies a UDP port number in the range of 1 to 65535.

Usage guidelines

The destination port in DAE packets on the DAC must be the same as the RADIUS DAS port on the DAS.

Examples

Enable the RADIUS DAS to listen to UDP port 3790 for DAE requests.

```
<Sysname> system-view
[Sysname] radius dynamic-author server
[Sysname-radius-da-server] port 3790
```

Related commands

client

radius dynamic-author server

primary accounting (RADIUS scheme view)

Use **primary accounting** to specify the primary RADIUS accounting server.

Use **undo primary accounting** to restore the default.

Syntax

primary accounting { *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **weight** *weight-value*] *

undo primary accounting

Default

The primary RADIUS accounting server is not specified.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

host-name: Specifies the host name of the primary RADIUS accounting server, a case-insensitive string of 1 to 253 characters.

ipv4-address: Specifies the IPv4 address of the primary RADIUS accounting server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the primary RADIUS accounting server.

port-number: Specifies the service port number of the primary RADIUS accounting server. The value range for the UDP port number is 1 to 65535. The default setting is 1813.

key: Specifies the shared key for secure communication with the primary RADIUS accounting server.

cipher: Specifies the key in encrypted form.

simple: Specifies the key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive. In non-FIPS mode, the encrypted form of the key is a string of 1 to 117 characters. The plaintext form of the key is a string of 1 to 64 characters. In FIPS mode, the encrypted form of the key is a string of 15 to 117 characters. The plaintext form of the key is a string of 15 to 64 characters. The plaintext string must contain digits, uppercase letters, lowercase letters, and special characters.

weight *weight-value*: Specifies a weight value for the RADIUS server. The value range for the *weight-value* argument is 0 to 100, and the default value is 0. The value **0** indicates that the RADIUS server will not be used for load sharing. This option takes effect only when the RADIUS server load sharing feature is enabled for the RADIUS scheme. A larger weight value represents a higher capacity to process accounting requests.

Usage guidelines

Make sure the port number and shared key settings of the primary RADIUS accounting server are the same as those configured on the server.

Two accounting servers specified for a scheme, primary or secondary, cannot have identical host name, IP address, and port number settings.

The shared key configured by using this command takes precedence over the shared key configured with the **key accounting** command.

If you use the **primary accounting** command to modify or delete the primary accounting server to which the device is sending a start-accounting request, communication with the primary server times out.

- When the RADIUS server load sharing feature is disabled, the device tries to communicate with an active server that has the highest priority for accounting.
- When the RADIUS server load sharing feature is enabled, the device returns an accounting failure message rather than searching for another active accounting server.

If you remove an actively used accounting server, the device no longer sends users' real-time accounting requests and stop-accounting requests. It does not buffer the stop-accounting requests. The device can generate incorrect accounting results.

Examples

In RADIUS scheme **radius1**, specify the primary accounting server with IP address 10.110.1.2, UDP port number 1813, and plaintext shared key **123456TESTacct&!**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] primary accounting 10.110.1.2 1813 key simple 123456TESTacct&!
```

Related commands

display radius scheme

key (RADIUS scheme view)

secondary accounting (RADIUS scheme view)

server-load-sharing enable

primary authentication (RADIUS scheme view)

Use **primary authentication** to specify the primary RADIUS authentication server.

Use **undo primary authentication** to restore the default.

Syntax

primary authentication { *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **test-profile** *profile-name* | **weight** *weight-value*] *

undo primary authentication

Default

The primary RADIUS authentication server is not specified.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

host-name: Specifies the host name of the primary RADIUS authentication server, a case-insensitive string of 1 to 253 characters.

ipv4-address: Specifies the IPv4 address of the primary RADIUS authentication server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the primary RADIUS authentication server.

port-number: Specifies the service port number of the primary RADIUS authentication server. The value range for the UDP port number is 1 to 65535. The default setting is 1812.

key: Specifies the shared key for secure communication with the primary RADIUS authentication server.

cipher: Specifies the key in encrypted form.

simple: Specifies the key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive. In non-FIPS mode, the encrypted form of the key is a string of 1 to 117 characters. The plaintext form of the key is a string of 1 to 64 characters. In FIPS mode, the encrypted form of the key is a string of 15 to 117 characters. The plaintext form of the key is a string of 15 to 64 characters. The plaintext string must contain digits, uppercase letters, lowercase letters, and special characters.

test-profile *profile-name*: Specifies a test profile for detecting the RADIUS server status. The *profile-name* argument is a case-sensitive string of 1 to 31 characters.

weight *weight-value*: Specifies a weight value for the RADIUS server. The value range for the *weight-value* argument is 0 to 100, and the default value is 0. The value **0** indicates that the RADIUS server will not be used for load sharing. This option takes effect only when the RADIUS server load sharing feature is enabled for the RADIUS scheme. A larger weight value represents a higher capacity to process authentication requests.

Usage guidelines

Make sure the service port and shared key settings of the primary RADIUS authentication server are the same as those configured on the server.

Two authentication servers specified for a scheme, primary or secondary, cannot have identical host name, IP address, and port number settings.

The shared key configured by this command takes precedence over the shared key configured with the **key authentication** command.

The server status detection is triggered for the server if the specified test profile exists on the device.

If you use the **primary authentication** command to modify or delete the primary authentication server during an authentication process, communication with the primary server times out.

- When the RADIUS server load sharing feature is disabled, the device tries to communicate with an active server that has the highest priority for authentication.
- When the RADIUS server load sharing feature is enabled, the device performs the following operations:
  a. Checks the weight value and number of currently served users for each active server.
  b. Determines the most appropriate server in performance to receive an AAA request.

Examples

In RADIUS scheme **radius1**, specify the primary authentication server with IP address 10.110.1.1, UDP port number 1812, and plaintext shared key **123456TESTauth&!**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] primary authentication 10.110.1.1 1812 key simple
123456TESTauth&!
```

Related commands

display radius scheme

key (RADIUS scheme view)

radius-server test-profile

secondary authentication (RADIUS scheme view)

server-load-sharing enable

radius attribute extended

Use **radius attribute extended** to define an extended RADIUS attribute.

Use **undo radius attribute extended** to delete user-defined extended RADIUS attributes.

Syntax

radius attribute extended *attribute-name* [**vendor** *vendor-id*] **code** *attribute-code* **type** { **binary** | **date** | **integer** | **interface-id** | **ip** | **ipv6** | **ipv6-prefix** | **octets** | **string** }

undo radius attribute extended [*attribute-name*]

Default

No user-defined extended RADIUS attributes exist.

Views

System view

Predefined user roles

network-admin

Parameters

attribute-name: Specifies the RADIUS attribute name, a case-insensitive string of 1 to 63 characters. The name must be unique among all RADIUS attributes, including the standard and extended RADIUS attributes.

vendor *vendor-id*: Specifies a vendor ID in the range of 1 to 65535. If you do not specify a vendor ID, the device processes the RADIUS attribute as a standard RADIUS attribute.

code *attribute-code*: Specifies the ID of the RADIUS attribute in the attribute set. The value range for the *attribute-code* argument is 1 to 255.

type: Specifies a data type for the attribute content.

binary: Binary type.

date: Date type.

integer: Integer type.

interface-id: Interface ID type.

ip: IPv4 address type.

ipv6: IPv6 address type.

ipv6-prefix: IPv6 address prefix type.

octets: Octet type.

string: String type.

Usage guidelines

To support the proprietary RADIUS attributes of other vendors, perform the following tasks:

1. Use this command to define the attributes as extended RADIUS attributes.
2. Use the **attribute convert** command to map the extended RADIUS attributes to attributes supported by the system.
3. Use the **attribute translate** command to enable the RADIUS attribute translation feature for the mappings to take effect.

To cooperate with RADIUS servers of a third-party vendor, map attributes that cannot be identified by the server to server-supported attributes.

Two RADIUS attributes cannot have the same combination of attribute name, vendor ID, and attribute ID.

If you do not specify a RADIUS attribute name, the **undo radius attribute extended** command deletes all user-defined extended RADIUS attributes.

Examples

Define a string-type extended RADIUS attribute with attribute name **Owner-Password**, vendor ID 122, and attribute ID 80.

```
<Sysname> system-view
[Sysname] radius attribute extended Owner-Password vendor 122 code 80 type string
```

Related commands

attribute convert (RADIUS DAS view)

attribute convert (RADIUS scheme view)

attribute reject (RADIUS DAS view)

attribute reject (RADIUS scheme view)

attribute translate

radius attribute-test-group

Use **radius attribute-test-group** to create a RADIUS attribute test group and enter its view, or enter the view of an existing RADIUS attribute test group.

Use **undo radius attribute-test-group** to remove a RADIUS attribute test group.

Syntax

radius attribute-test-group *attr-test-group-name*

undo radius attribute-test-group *attr-test-group-name*

Default

No RADIUS attribute test groups exist.

Views

System view

Predefined user roles

network-admin

Parameters

attr-test-group-name: Specifies the name of a RADIUS attribute test group, a case-insensitive string of 1 to 31 characters.

Usage guidelines

A RADIUS attribute test group is a collection of RADIUS attributes that will be included in or excluded from RADIUS requests.

The system can have multiple RADIUS attribute test groups.

Examples

Create a RADIUS attribute test group named **t1** and enter its view.

```
<Sysname> system-view
[Sysname] radius attribute-test-group t1
[Sysname-radius-attr-test-grp-t1]
```

Related commands

exclude

include

test-aaa

radius dscp

Use **radius dscp** to change the DSCP priority of RADIUS packets.

Use **undo radius dscp** to restore the default.

Syntax

radius [**ipv6**] **dscp** *dscp-value*

undo radius [**ipv6**] **dscp**

Default

The DSCP priority of RADIUS packets is 0.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6: Specifies the IPv6 RADIUS packets. If you do not specify this keyword, the command sets the DSCP priority for the IPv4 RADIUS packets.

dscp-value: Specifies the DSCP priority of RADIUS packets, in the range of 0 to 63. A larger value represents a higher priority.

Usage guidelines

Use this command to set the DSCP priority in the ToS field of RADIUS packets for changing their transmission priority.

Examples

Set the DSCP priority of IPv4 RADIUS packets to 10.

```
<Sysname> system-view
[Sysname] radius dscp 10
```

radius dynamic-author server

Use **radius dynamic-author server** to enable the RADIUS DAS feature and enter RADIUS DAS view.

Use **undo radius dynamic-author server** to disable the RADIUS DAS feature.

Syntax

radius dynamic-author server

undo radius dynamic-author server

Default

The RADIUS DAS feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

After you enable the RADIUS DAS feature, the device listens to the RADIUS DAS port to receive DAE packets from specified DACs. Based on the DAE packet type and contents, the device performs one of the following operations:

- Log off online users.
- Change online user authorization information.
- Shut down or reboot online users' access ports.
- Reauthenticate online users.

Examples

Enable the RADIUS DAS feature and enter RADIUS DAS view.

```
<Sysname> system-view
[Sysname] radius dynamic-author server
[Sysname-radius-da-server]
```

Related commands

client

port

radius enable

Use **radius enable** to enable the RADIUS service.

Use **undo radius enable** to disable the RADIUS service.

Syntax

radius enable

undo radius enable

Default

The RADIUS service is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

By default, the RADIUS service is enabled. The device can send and receive RADIUS packets. Attackers might use RADIUS session-control and DAE ports to attack the device. To protect the device when such an attack occurs, disable the RADIUS service temporarily on the device. After the network is secure, re-enable the RADIUS service.

If settings on the RADIUS servers require modification or the RADIUS servers cannot provide services temporarily, you can temporarily disable the RADIUS service on the device.

When the RADIUS service is disabled, the device stops sending and receiving RADIUS packets. If a new user comes online, the device uses the backup authentication, authorization, or accounting method to process that user. If the device has not finished requesting authentication or accounting for a user before the RADIUS service is disabled, it uses the following rules to process that user:

- If the device has sent RADIUS authentication requests for that user to a RADIUS server, the device processes that user depending on whether it receives a response from the RADIUS server.
  - If the device receives a response from the RADIUS server, it uses the response to determine whether that user has passed authentication. If that user has passed authentication, the device assigns authorization information to that user according to the response.
  - If the device does not receive any response from the RADIUS server, it attempts to use the backup authentication method to authenticate that user.
- If the device has sent RADIUS start-accounting requests for that user to a RADIUS server, the device processes that user depending on whether it receives a response from the RADIUS server.
  - If the device receives a response from the RADIUS server, it allows that user to come online. However, the device cannot send out accounting-update or stop-accounting requests to the RADIUS server. It cannot buffer the accounting requests, either. When that user goes offline, the RADIUS server cannot log off that user in time. The accounting result might be inaccurate.
  - If the device does not receive any response from the RADIUS server, it attempts to use the backup accounting method.

Disabling the RADIUS service does not affect the RADIUS server feature of the device.

The authentication, authorization, and accounting processes undertaken by other methods are not switched to RADIUS when you re-enable the RADIUS service.

Examples

Enable the RADIUS service.

```
<Sysname> system-view
[Sysname] radius enable
```

radius nas-ip

Use **radius nas-ip** to specify a source interface or source IP address for outgoing RADIUS packets.

Use **undo radius nas-ip** to delete the specified source interface or source IP address for outgoing RADIUS packets.

Syntax

radius nas-ip { **interface** *interface-type interface-number* | { *ipv4-address* | **ipv6** *ipv6-address* } }

undo radius nas-ip { **interface** | { *ipv4-address* | **ipv6** *ipv6-address* } }

Default

The source IP address of an outgoing RADIUS packet is the primary IPv4 address or the IPv6 address of the outbound interface.

Views

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a source interface by its type and number. The device uses the primary IPv4 address or the IPv6 address of the interface as the source IP address of an outgoing RADIUS packet.

ipv4-address: Specifies an IPv4 address, which must be an address of the device. The IP address cannot be 0.0.0.0, 255.255.255.255, a class D address, a class E address, or a loopback address.

ipv6 *ipv6-address*: Specifies an IPv6 address, which must be a unicast address of the device and cannot be a loopback address or a link-local address.

Usage guidelines

The source IP address of RADIUS packets that a NAS sends must match the IP address of the NAS that is configured on the RADIUS server. A RADIUS server identifies a NAS by its IP address. Upon receiving a RADIUS packet, the RADIUS server checks the source IP address of the packet.

- If the source IP address of the packet is the IP address of a managed NAS, the server processes the packet.
- If the source IP address of the packet is not the IP address of a managed NAS, the server drops the packet.

As a best practice, specify a loopback interface address as the source IP address for outgoing RADIUS packets to avoid RADIUS packet loss caused by physical port errors.

If you use both the **nas-ip** command and **radius nas-ip** command, the following guidelines apply:

- The setting configured by using the **nas-ip** command in RADIUS scheme view applies only to the RADIUS scheme.
- The setting configured by using the **radius nas-ip** command in system view applies to all RADIUS schemes.
- The setting in RADIUS scheme view takes precedence over the setting in system view.

You can specify only one source IPv4 address and one source IPv6 address in system view.

You can specify only one source interface to provide the source IP address for outgoing RADIUS packets. Make sure the route between the source interface and the RADIUS server is reachable.

The source interface configuration and the source IP address configuration overwrite each other.

Examples

Specify IP address 129.10.10.1 as the source IP address for outgoing RADIUS packets.

```
<Sysname> system-view
[Sysname] radius nas-ip 129.10.10.1
```

Related commands

nas-ip (RADIUS scheme view)

radius scheme

Use **radius scheme** to create a RADIUS scheme and enter its view, or enter the view of an existing RADIUS scheme.

Use **undo radius scheme** to delete a RADIUS scheme.

Syntax

radius scheme *radius-scheme-name*

undo radius scheme *radius-scheme-name*

Default

No RADIUS schemes exist.

Views

System view

Predefined user roles

network-admin

Parameters

radius-scheme-name: Specifies the RADIUS scheme name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

A RADIUS scheme can be used by more than one ISP domain at the same time.

The device supports a maximum of 16 RADIUS schemes.

Examples

Create a RADIUS scheme named **radius1** and enter RADIUS scheme view.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1]
```

Related commands

display radius scheme

radius session-control client

Use **radius session-control client** to specify a RADIUS session-control client.

Use **undo radius session-control client** to remove the specified RADIUS session-control clients.

Syntax

radius session-control client { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**key** { **cipher** | **simple** } *string*]

undo radius session-control client { **all** | { **ip** *ipv4-address* | **ipv6** *ipv6-address* } }

Default

No RADIUS session-control clients are specified.

Views

System view

Predefined user roles

network-admin

Parameters

ip *ipv4-address*: Specifies a session-control client by its IPv4 address.

ipv6 *ipv6-address*: Specifies a session-control client by its IPv6 address.

key: Specifies the shared key for secure communication with the session-control client.

cipher: Specifies the key in encrypted form.

simple: Specifies the key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive. In non-FIPS mode, the encrypted form of the key is a string of 1 to 117 characters. The plaintext form of the key is a string of 1 to 64 characters. In FIPS mode, the encrypted form of the key is a string of 15 to 117 characters. The plaintext form of the key is a string of 15 to 64 characters. The plaintext string must contain digits, uppercase letters, lowercase letters, and special characters.

all: Specifies all session-control clients.

Usage guidelines

To verify the session-control packets sent from a RADIUS server running on IMC, specify the RADIUS server as a session-control client to the device. The device matches a session-control packet to a session-control client based on the IP address, and then uses the shared key of the matched client to validate the packet.

The device searches the session-control client settings prior to searching all RADIUS scheme settings for a server with matching settings. This process narrows the search scope for finding the matched RADIUS server.

The session-control client settings take effect only when the RADIUS session-control feature is enabled.

The session-control client settings must be the same as the corresponding settings of the RADIUS server.

You can specify multiple session-control clients on the device.

Examples

Specify a session-control client with IP address 10.110.1.2 and shared key **12345** in plaintext form.

```
<Sysname> system-view
[Sysname] radius session-control client ip 10.110.1.2 key simple 12345
```

Related commands

radius session-control enable

radius session-control enable

Use **radius session-control enable** to enable the RADIUS session-control feature.

Use **undo radius session-control enable** to disable the RADIUS session-control feature.

Syntax

radius session-control enable

undo radius session-control enable

Default

The RADIUS session-control feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

An H3C IMC RADIUS server uses session-control packets to change the user authorization information (such as the authorization ACL, VLAN, and user group) or forcibly disconnect users. The session-control feature enables the device to receive the RADIUS session-control packets on UDP port 1812.

This feature must work with H3C IMC servers.

If the device acts as the NAS and the IMC server deployed with EAD assigns authorization ACLs to the device, you must enable the session-control feature on the device. This ensures that the authorization ACLs can take effect.

Examples

Enable the RADIUS session-control feature.

```
<Sysname> system-view
[Sysname] radius session-control enable
```

radius-server test-profile

Use **radius-server test-profile** to configure a test profile for detecting the RADIUS server status.

Use **undo radius-server test-profile** to delete a RADIUS test profile.

Syntax

radius-server test-profile *profile-name* **username** *name* [**password** { **cipher** | **simple** } *string*] [**interval** *interval*] [**eap-profile** *eap-profile-name*]

undo radius-server test-profile *profile-name*

Default

No RADIUS test profiles exist.

Views

System view

Predefined user roles

network-admin

Parameters

profile-name: Specifies the name of the test profile, which is a case-sensitive string of 1 to 31 characters.

username *name*: Specifies the username in the detection packets. The *name* argument is a case-sensitive string of 1 to 253 characters.

password: Specifies the user password in the detection packets. If you do not specify a user password, the device randomly generates a user password for each detection packet. As a best practice, specify a user password. RADIUS server might mistake detection packets that contain randomly generated passwords as attack packets.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 63 characters. Its encrypted form is a case-sensitive string of 1 to 117 characters.

interval *interval*: Specifies the interval for sending a detection packet, in minutes. The value range for the *interval* argument is 1 to 3600, and the default value is 60.

eap-profile *eap-profile-name*: Specifies an EAP profile by its name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

The device starts detecting the status of a RADIUS server only if the test profile specified for the server exists. If you specify a nonexistent test profile for a RADIUS server, the device does not detect the status of the server until you create the test profile on the device.

To perform EAP-based status detection for a RADIUS server, you must specify a test profile that contains an EAP profile for the RADIUS server.

EAP-based detection provides more reliable detection results than simple detection. As a best practice, configure EAP-based detection on a network environment where EAP authentication is configured.

If you specify a nonexistent EAP profile in a test profile, the device performs simple detection for the RADIUS servers that use the test profile. After the EAP profile is configured, the device will start EAP-based detection at the next detection interval.

When you delete a test profile, the device stops detecting the status of RADIUS servers that use the test profile.

You can execute this command multiple times to configure multiple test profiles.

Examples

Configure a test profile named **abc** for RADIUS server status detection. A detection packet that uses username **admin** and plaintext password **abc123** is sent every 10 minutes.

```
<Sysname> system-view
[Sysname] radius-server test-profile abc username admin password simple abc123 interval
10
```

Related commands

eap-profile

primary authentication (RADIUS scheme view)

secondary authentication (RADIUS scheme view)

reset radius server-load statistics

Use **reset radius server-load statistics** to clear history authentication and accounting load statistics for all RADIUS servers.

Syntax

reset radius server-load statistics

Views

User view

Predefined user roles

network-admin

Usage guidelines

This command does not clear authentication and accounting load statistics in the last 5 seconds.

Examples

Clear history authentication and accounting load statistics for all RADIUS servers.

```
<Sysname> reset radius server-load statistics
```

Related commands

display radius server-load statistics

reset radius statistics

Use **reset radius statistics** to clear RADIUS statistics.

Syntax

reset radius statistics

Views

User view

Predefined user roles

network-admin

Examples

Clear RADIUS statistics.

```
<Sysname> reset radius statistics
```

Related commands

display radius statistics

reset stop-accounting-buffer (for RADIUS)

Use **reset stop-accounting-buffer** to clear buffered RADIUS stop-accounting requests to which no responses have been received.

Syntax

reset stop-accounting-buffer { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time end-time* | **user-name** *user-name* }

Views

User view

Predefined user roles

network-admin

Parameters

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

session-id *session-id*: Specifies a session by its ID. The *session-id* argument is a string of 1 to 64 characters and cannot contain a letter. A session ID uniquely identifies an online user for a RADIUS scheme.

time-range *start-time end-time*: Specifies a time range. The start time and end time must be in the format of hh:mm:ss-mm/dd/yyyy or hh:mm:ss-yyyy/mm/dd.

user-name *user-name*: Specifies a user by its name, a case-sensitive string of 1 to 255 characters. Whether the *user-name* argument should include the domain name depends on the setting configured by using the **user-name-format** command for the RADIUS scheme.

Examples

Clear nonresponded RADIUS stop-accounting requests buffered for user **user0001@test**.

```
<Sysname> reset stop-accounting-buffer user-name user0001@test
```

Clear nonresponded RADIUS stop-accounting requests buffered from 0:0:0 to 23:59:59 on August 31, 2015.

```
<Sysname> reset stop-accounting-buffer time-range 0:0:0-08/31/2015 23:59:59-08/31/2015
```

Related commands

display stop-accounting-buffer (for RADIUS)

stop-accounting-buffer enable (RADIUS scheme view)

retry

Use **retry** to set the maximum number of attempts for transmitting a RADIUS packet to a single RADIUS server.

Use **undo retry** to restore the default.

Syntax

retry *retries*

undo retry

Default

The maximum number of RADIUS packet transmission attempts is 3.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

retries: Specifies the maximum number of RADIUS packet transmission attempts, in the range of 1 to 20.

Usage guidelines

Because RADIUS uses UDP packets to transmit data, the communication is not reliable.

If the device does not receive a response to its request from the RADIUS server within the response timeout period, the device retransmits the RADIUS request. To set the response timeout period, use the **timer response-timeout** command.

If the device does not receive a response from the RADIUS server after the maximum number of transmission attempts is reached, the device considers the request a failure.

If the client times out during the authentication process, the user is immediately logged off. To avoid user logoffs, the value multiplied by the following items cannot be larger than the client timeout period defined by the access module:

- The maximum number of RADIUS packet transmission attempts.
- The RADIUS server response timeout period.
- The number of RADIUS authentication servers in the RADIUS scheme.

When the device sends a RADIUS request to a new RADIUS server, it checks the total amount of time it has taken to transmit the RADIUS packet. If the amount of time has reached 300 seconds, the device stops sending the RADIUS request to the next RADIUS server. As a best practice, consider the number of RADIUS servers when you configure the maximum number of packet transmission attempts and the RADIUS server response timeout period.

Examples

In RADIUS scheme **radius1**, set the maximum number of RADIUS packet transmission attempts to 5.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] retry 5
```

Related commands

radius scheme

timer response-timeout (RADIUS scheme view)

retry realtime-accounting

Use **retry realtime-accounting** to set the maximum number of accounting attempts.

Use **undo retry realtime-accounting** to restore the default.

Syntax

retry realtime-accounting *retries*

undo retry realtime-accounting

Default

The maximum number of accounting attempts is 5.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

retries: Specifies the maximum number of accounting attempts, in the range of 1 to 255.

Usage guidelines

Typically, a RADIUS accounting server checks whether a user is online by using a timeout timer. If the server does not receive a real-time accounting request for a user in the timeout period, it considers that a line or device failure has occurred. The server stops accounting for the user.

To work with the RADIUS server, the NAS needs to send real-time accounting requests to the server before the timer on the server expires and to keep pace with the server in disconnecting the user

when a failure occurs. The NAS disconnects from a user according to the maximum number of accounting attempts and specific parameters.

For example, the following conditions exist:

- The RADIUS server response timeout period is 3 seconds (set by using the **timer response-timeout** command).
- The maximum number of RADIUS packet transmission attempts is 3 (set by using the **retry** command).
- The real-time accounting interval is 12 minutes (set by using the **timer realtime-accounting** command).
- The maximum number of accounting attempts is 5 (set by using the **retry realtime-accounting** command).

In the above case, the device generates an accounting request every 12 minutes, and retransmits the request if it sends the request but receives no response within 3 seconds. If the device receives no response after transmitting the request three times, it considers the accounting attempt a failure, and makes another accounting attempt. If five consecutive accounting attempts fail, the device cuts the user connection.

Examples

In RADIUS scheme **radius1**, set the maximum number of accounting attempts to 10.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] retry realtime-accounting 10
```

Related commands

retry

timer realtime-accounting (RADIUS scheme view)

timer response-timeout (RADIUS scheme view)

retry stop-accounting (RADIUS scheme view)

Use **retry stop-accounting** to set the maximum number of transmission attempts for individual RADIUS stop-accounting requests.

Use **undo retry stop-accounting** to restore the default.

Syntax

retry stop-accounting *retries*

undo retry stop-accounting

Default

The maximum number of transmission attempts is 500 for individual RADIUS stop-accounting requests.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

retries: Specifies the maximum number of transmission attempts. The value range is 10 to 65535.

Usage guidelines

The maximum number of stop-accounting request transmission attempts controls the transmission of stop-accounting requests together with the following parameters:

- RADIUS server response timeout timer (set by using the **timer response-timeout** command).
- Maximum number of times to transmit a RADIUS packet per round (set by using the **retry** command).

For example, the following settings exist:

- The RADIUS server response timeout timer is 3 seconds.
- The maximum number of times to transmit a RADIUS packet per round is five.
- The maximum number of stop-accounting request transmission attempts is 20.

A stop-accounting request is retransmitted if the device does not receive a response within 3 seconds. When all five transmission attempts in this round are used, the device buffers the request and starts another round of retransmission. If 20 consecutive rounds of attempts fail, the device discards the request.

Examples

Set the maximum number of stop-accounting request transmission attempts to 1000 for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] retry stop-accounting 1000
```

Related commands

display stop-accounting-buffer (for RADIUS)

retry

timer response-timeout (RADIUS scheme view)

secondary accounting (RADIUS scheme view)

Use **secondary accounting** to specify a secondary RADIUS accounting server.

Use **undo secondary accounting** to remove a secondary RADIUS accounting server.

Syntax

secondary accounting { *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **weight** *weight-value*] *

undo secondary accounting [{ *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number*]]

Default

No secondary RADIUS accounting servers are specified.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

host-name: Specifies the host name of a secondary RADIUS accounting server, a case-insensitive string of 1 to 253 characters.

ipv4-address: Specifies the IPv4 address of a secondary RADIUS accounting server.

ipv6 *ipv6-address*: Specifies the IPv6 address of a secondary RADIUS accounting server.

port-number: Specifies the service port number of the secondary RADIUS accounting server. The value range for the UDP port number is 1 to 65535. The default setting is 1813.

key: Specifies the shared key for secure communication with the secondary RADIUS accounting server.

cipher: Specifies the key in encrypted form.

simple: Specifies the key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive. In non-FIPS mode, the encrypted form of the key is a string of 1 to 117 characters. The plaintext form of the key is a string of 1 to 64 characters. In FIPS mode, the encrypted form of the key is a string of 15 to 117 characters. The plaintext form of the key is a string of 15 to 64 characters. The plaintext string must contain digits, uppercase letters, lowercase letters, and special characters.

weight *weight-value*: Specifies a weight value for the RADIUS server. The value range for the *weight-value* argument is 0 to 100, and the default value is 0. The value **0** indicates that the RADIUS server will not be used for load sharing. This option takes effect only when the RADIUS server load sharing feature is enabled for the RADIUS scheme. A larger weight value represents a higher capacity to process accounting requests.

Usage guidelines

Make sure the port number and shared key settings of each secondary RADIUS accounting server are the same as those configured on the corresponding server.

A RADIUS scheme supports a maximum of 16 secondary RADIUS accounting servers. If the primary server fails, the device tries to communicate with a secondary server in active state. The device connects to the secondary servers in the order they are configured.

Two accounting servers specified for a scheme, primary or secondary, cannot have identical host name, IP address, and port number settings.

The shared key configured by this command takes precedence over the shared key configured with the **key accounting** command.

If you use the **secondary accounting** command to modify or delete a secondary accounting server to which the device is sending a start-accounting request, communication with the secondary server times out.

- When the RADIUS server load sharing feature is disabled, the device tries to communicate with an active server that has the highest priority for accounting.
- When the RADIUS server load sharing feature is enabled, the device returns an accounting failure message rather than searching for another active accounting server.

If you remove an actively used accounting server, the device no longer sends users' real-time accounting requests and stop-accounting requests. The device does not buffer the stop-accounting requests, either.

Examples

In RADIUS scheme **radius1**, specify a secondary accounting server with IP address 10.110.1.1 and UDP port 1813.

```
<Sysname> system-view
[Sysname] radius scheme radius1
```

```
[Sysname-radius-radius1] secondary accounting 10.110.1.1 1813
```

In RADIUS scheme **radius2**, specify two secondary accounting servers with IP addresses 10.110.1.1 and 10.110.1.2 and UDP port 1813.

```
<Sysname> system-view
[Sysname] radius scheme radius2
[Sysname-radius-radius2] secondary accounting 10.110.1.1 1813
[Sysname-radius-radius2] secondary accounting 10.110.1.2 1813
```

Related commands

display radius scheme

key (RADIUS scheme view)

primary accounting (RADIUS scheme view)

secondary authentication (RADIUS scheme view)

Use **secondary authentication** to specify a secondary RADIUS authentication server.

Use **undo secondary authentication** to remove a secondary RADIUS authentication server.

Syntax

secondary authentication { *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **test-profile** *profile-name* | **weight** *weight-value*] *

undo secondary authentication [{ *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number*]]

Default

No secondary RADIUS authentication servers are specified.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

host-name: Specifies the host name of a secondary RADIUS authentication server, a case-insensitive string of 1 to 253 characters.

ipv4-address: Specifies the IPv4 address of a secondary RADIUS authentication server.

ipv6 *ipv6-address*: Specifies the IPv6 address of a secondary RADIUS authentication server.

port-number: Specifies the service port number of the secondary RADIUS authentication server. The value range for the UDP port number is 1 to 65535. The default setting is 1812.

key: Specifies the shared key for secure communication with the secondary RADIUS authentication server.

cipher: Specifies the key in encrypted form.

simple: Specifies the key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive. In non-FIPS mode, the encrypted form of the key is a string of 1 to 117 characters. The plaintext form of the key is a string of 1 to 64 characters. In FIPS mode, the encrypted form of the key is a string of 15 to 117 characters. The

plaintext form of the key is a string of 15 to 64 characters. The plaintext string must contain digits, uppercase letters, lowercase letters, and special characters.

test-profile *profile-name*: Specifies a test profile for detecting the RADIUS server status. The *profile-name* argument is a case-sensitive string of 1 to 31 characters.

weight *weight-value*: Specifies a weight value for the RADIUS server. The value range for the *weight-value* argument is 0 to 100, and the default value is 0. The value **0** indicates that the RADIUS server will not be used for load sharing. This option takes effect only when the RADIUS server load sharing feature is enabled for the RADIUS scheme. A larger weight value represents a higher capacity to process authentication requests.

Usage guidelines

Make sure the port number and shared key settings of each secondary RADIUS authentication server are the same as those configured on the corresponding server.

A RADIUS scheme supports a maximum of 16 secondary RADIUS authentication servers. If the primary server fails, the device tries to communicate with a secondary server in active state. The device connects to the secondary servers in the order they are configured.

The server status detection is triggered for a server if the specified test profile exists on the device.

Two authentication servers specified for a scheme, primary or secondary, cannot have identical host name, IP address, and port number settings.

The shared key configured by this command takes precedence over the shared key configured with the **key authentication** command.

If you use the **secondary authentication** command to modify or delete a secondary authentication server during an authentication process, communication with the secondary server times out.

- When the RADIUS server load sharing feature is disabled, the device tries to communicate with an active server that has the highest priority for authentication.
- When the RADIUS server load sharing feature is enabled, the device performs the following operations:
  a. Checks the weight value and number of currently served users for each active server.
  b. Determines the most appropriate server in performance to receive an AAA request.

Examples

In RADIUS scheme **radius1**, specify a secondary authentication server with IP address 10.110.1.2 and UDP port 1812.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] secondary authentication 10.110.1.2 1812
```

In RADIUS scheme **radius2**, specify two secondary authentication servers with IP addresses 10.110.1.1 and 10.110.1.2 and UDP port 1812.

```
<Sysname> system-view
[Sysname] radius scheme radius2
[Sysname-radius-radius2] secondary authentication 10.110.1.1 1812
[Sysname-radius-radius2] secondary authentication 10.110.1.2 1812
```

Related commands

display radius scheme

key (RADIUS scheme view)

primary authentication (RADIUS scheme view)

radius-server test-profile

server-load-sharing enable

Use **server-load-sharing enable** to enable the RADIUS server load sharing feature.

Use **undo server-load-sharing enable** to disable the RADIUS server load sharing feature.

Syntax

server-load-sharing enable

undo server-load-sharing enable

Default

The RADIUS server load sharing feature is disabled.

Views

RADIUS scheme view

Predefined user roles

network-admin

Usage guidelines

Use the RADIUS server load sharing feature to dynamically distribute the workload over multiple servers regardless of their server roles. The device forwards an AAA request to the most appropriate server of all active servers in the scheme after it compares the weight values and numbers of currently served users. Specify a weight value for each RADIUS server based on the AAA capacity of the server. A larger weight value indicates a higher AAA capacity.

In RADIUS server load sharing, once the device sends a start-accounting request to a server for a user, it forwards all subsequent accounting requests of the user to the same server. If the accounting server is unreachable, the device returns an accounting failure message rather than searching for another active accounting server.

Examples

Enable the RADIUS server load sharing feature for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] server-load-sharing enable
```

Related commands

primary authentication (RADIUS scheme view)

primary accounting (RADIUS scheme view)

secondary authentication (RADIUS scheme view)

secondary accounting (RADIUS scheme view)

snmp-agent trap enable radius

Use **snmp-agent trap enable radius** to enable SNMP notifications for RADIUS.

Use **undo snmp-agent trap enable radius** to disable SNMP notifications for RADIUS.

Syntax

snmp-agent trap enable radius [**accounting-server-down** | **accounting-server-up** | **authentication-error-threshold** | **authentication-server-down** | **authentication-server-up**] *

undo snmp-agent trap enable radius [**accounting-server-down** | **accounting-server-up** | **authentication-error-threshold** | **authentication-server-down** | **authentication-server-up**] *

Default

All RADIUS SNMP notifications are disabled.

Views

System view

Predefined user roles

network-admin

Parameters

accounting-server-down: Specifies notifications to be sent when the RADIUS accounting server becomes unreachable.

accounting-server-up: Specifies notifications to be sent when the RADIUS accounting server becomes reachable.

authentication-error-threshold: Specifies notifications to be sent when the number of authentication failures exceeds the specified threshold. The threshold is represented by the ratio of the authentication failures to the total number of authentication attempts. The value range is 1 to 100, and the default value is 30. This threshold can only be configured through the MIB.

authentication-server-down: Specifies notifications to be sent when the RADIUS authentication server becomes unreachable.

authentication-server-up: Specifies notifications to be sent when the RADIUS authentication server becomes reachable.

Usage guidelines

If you do not specify any keywords, this command enables or disables all types of notifications for RADIUS.

When SNMP notifications for RADIUS are enabled, the device supports the following notifications generated by RADIUS:

- **RADIUS server unreachable notification**—The RADIUS server cannot be reached. RADIUS generates this notification if it cannot receive any response to an accounting or authentication request within the specified RADIUS request transmission attempts.
- **RADIUS server reachable notification**—The RADIUS server can be reached. RADIUS generates this notification for a previously blocked RADIUS server after the quiet timer expires.
- **Excessive authentication failures notification**—RADIUS generates this notification when the number of authentication failures to the total number of authentication attempts exceeds the specified threshold.

Examples

Enable the device to send RADIUS accounting server unreachable notifications.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable radius accounting-server-down
```

state primary

Use **state primary** to set the status of a primary RADIUS server.

Syntax

state primary { **accounting** | **authentication** } { **active** | **block** }

Default

A primary RADIUS server is in active state.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

accounting: Specifies the primary RADIUS accounting server.

authentication: Specifies the primary RADIUS authentication server.

active: Specifies the active state, the normal operation state.

block: Specifies the blocked state, the out-of-service state.

Usage guidelines

When the RADIUS server load sharing feature is disabled, the device first tries to communicate with the primary server if the primary server is in active state. If the primary server is unavailable, the device performs the following operations:

- Changes the status of the primary server to blocked.
- Starts a quiet timer for the server.
- Tries to communicate with a secondary server in active state.

When the quiet timer of the primary server times out, the status of the server automatically changes to active. If you set the server status to blocked before the quiet timer times out, the server status cannot change back to active unless you manually set the status to active.

When the RADIUS server load sharing feature is enabled, the device checks the weight value and number of currently served users only for servers in active state. The most appropriate active server is selected for communication.

When the primary server and all secondary servers are in blocked state, the device tries to communicate with the primary server.

This command can affect the RADIUS server status detection feature when a valid test profile is specified for a primary RADIUS authentication server.

- If you set the status of the server to blocked, the device stops detecting the status of the server.
- If you set the status of the server to active, the device starts to detect the status of the server.

Examples

In RADIUS scheme **radius1**, set the status of the primary authentication server to blocked.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] state primary authentication block
```

Related commands

display radius scheme

radius-server test-profile

server-load-sharing enable

state secondary

state secondary

Use **state secondary** to set the status of a secondary RADIUS server.

Syntax

state secondary { **accounting** | **authentication** } [{ *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number*]] { **active** | **block** }

Default

A secondary RADIUS server is in active state.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

accounting: Specifies a secondary RADIUS accounting server.

authentication: Specifies a secondary RADIUS authentication server.

host-name: Specifies the host name of the secondary RADIUS server, a case-insensitive string of 1 to 253 characters.

ipv4-address: Specifies the IPv4 address of a secondary RADIUS server.

ipv6 *ipv6-address*: Specifies the IPv6 address of a secondary RADIUS server.

port-number: Specifies the service port number of a secondary RADIUS server. The value range for the UDP port number is 1 to 65535. The default port numbers for authentication and accounting are 1812 and 1813, respectively.

active: Specifies the active state, the normal operation state.

block: Specifies the blocked state, the out-of-service state.

Usage guidelines

If you do not specify an IP address, this command changes the status of all configured secondary RADIUS servers.

If the device finds that a secondary server in active state is unreachable, the device performs the following operations:

- Changes the status of the secondary server to blocked.
- Starts a quiet timer for the server.
- Tries to communicate with another secondary server in active state.

When the quiet timer of a server times out, the status of the server automatically changes to active. If you set the server status to blocked before the quiet timer times out, the server status cannot change back to active unless you manually set the status to active. If all configured secondary servers are unreachable, the device considers the authentication or accounting attempt a failure.

When the RADIUS server load sharing feature is enabled, the device checks the weight value and number of currently served users only for servers in active state. The most appropriate active server is selected for communication.

This command can affect the RADIUS server status detection feature when a valid test profile is specified for a secondary RADIUS authentication server.

- If you set the status of the server to blocked, the device stops detecting the status of the server.
- If you set the status of the server to active, the device starts to detect the status of the server.

Examples

In RADIUS scheme **radius1**, set the status of all the secondary authentication servers to blocked.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] state secondary authentication block
```

Related commands

display radius scheme

radius-server test-profile

server-load-sharing enable

state primary

stop-accounting-buffer enable (RADIUS scheme view)

Use **stop-accounting-buffer enable** to enable buffering of RADIUS stop-accounting requests to which no responses have been received.

Use **undo stop-accounting-buffer enable** to disable the buffering feature.

Syntax

stop-accounting-buffer enable

undo stop-accounting-buffer enable

Default

The device buffers the RADIUS stop-accounting requests to which no responses have been received.

Views

RADIUS scheme view

Predefined user roles

network-admin

Usage guidelines

This command enables the device to buffer a RADIUS stop-accounting request that has no response after the maximum transmission attempts (set by using the **retry** command) have been made. The device resends the buffered request until it receives a server response or when the number of stop-accounting request transmission attempts reaches the upper limit. If no more attempts are available, the device discards the request. However, if you have removed an accounting server, stop-accounting requests destined for the server are not buffered.

Examples

Enable buffering of RADIUS stop-accounting requests to which no responses have been received.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] stop-accounting-buffer enable
```

Related commands

display stop-accounting-buffer (for RADIUS)

reset stop-accounting-buffer (for RADIUS)

stop-accounting-packet send-force

Use **stop-accounting-packet send-force** to enable forcibly sending stop-accounting packets. The device will send stop-accounting packets when users for which no start-accounting packets are sent go offline.

Use **undo stop-accounting-packet send-force** to disable forcibly sending stop-accounting packets.

Syntax

stop-accounting-packet send-force

undo stop-accounting-packet send-force

Default

Forcibly sending stop-accounting packets is disabled. The device does not send stop-accounting packets when users for which no start-accounting packets are sent go offline.

Views

RADIUS scheme view

Predefined user roles

network-admin

Usage guidelines

Typically, if the device does not send a start-accounting packet to the RADIUS server for an authenticated user, it does not send a stop-accounting packet when the user goes offline. If the server has generated a user entry for the user without start-accounting packets, it does not release the user entry when the user goes offline. This feature forces the device to send stop-accounting packets to the RADIUS server when the user goes offline for timely releasing the user entry on the server.

Examples

In RADIUS scheme **radius1**, enable forcibly sending stop-accounting packets.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] stop-accounting-packet send-force
```

Related commands

display radius scheme

test-aaa

Use **test-aaa** to perform an AAA test.

Syntax

test-aaa user *user-name* **password** *password* **radius-scheme** *radius-scheme-name* [**radius-server** { *ipv4-address* | **ipv6** *ipv6-address* } *port-number*] [**chap** | **pap**] [**attribute-test-group** attr-*test-group-name*] [**trace**]

Views

User view

Predefined user roles

network-admin

Parameters

user *user-name*: Specifies the test username, a string of 1 to 80 characters. The username can be a pure username or contain a domain name. The format for a username containing a domain name is *pure-username@domain-name*. The pure username is case sensitive and the domain name is case insensitive.

password *password*: Specifies the password of the test user, a case-sensitive string of 1 to 63 characters.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

radius-server: Specifies a RADIUS server.

ipv4-address: Specifies the IPv4 address of the RADIUS server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the RADIUS server.

port-number: Specifies the UDP port number of the RADIUS server, in the range of 1 to 65535.

chap: Specifies the CHAP authentication method (the default).

pap: Specifies the PAP authentication method.

attribute-test-group *attr-test-group-name*: Specifies a RADIUS attribute test group by its name, a case-insensitive string of 1 to 31 characters. If you do not specify a RADIUS attribute test group or the specified RADIUS attribute test group does not exist, the device does not change the attributes carried in authentication or accounting requests.

trace: Displays detailed information about RADIUS packets exchanged during the AAA test. If you do not specify this keyword, the command displays brief information about the AAA test, including the sent and received packets and the test result.

Usage guidelines

Use this command to identify the reasons for the failure of interaction between the device and the AAA servers.

The device might communicate with the AAA servers incorrectly during an AAA test. Make sure no users come online or go offline during an AAA text.

If the configuration of the specified RADIUS scheme changes, the new configuration does not affect the current AAA test. The modification will take effect in the next test.

The system can have only one AAA test at a time. Another AAA test can be performed only after the current test finishes.

Examples

Perform an AAA test and display detailed information about the test. The test uses username **user1**, password **123456**, the CHAP authentication method, and RADIUS scheme **test**.

```
<Sysname> test-aaa user user1 password 123456 radius-scheme test chap trace
Sent a RADIUS authentication request.
  Server  IP   : 192.168.1.110
  Source  IP   : 192.168.1.166
  VPN instance : N/A
  Server port  : 1812
  Packet type  : Authentication request
  Packet length: 118 bytes
  Packet ID    : 0
  Attribute list:
    [User-Name(1)]                [6]   [user1]
    [CHAP-Password(3)]            [19]  [******]
```

```
    [NAS-IP-Address(4)]            [6]   [192.168.1.166]
    [Service-Type(6)]              [6]   [2] [Framed]
    [Framed-Protocol(7)]           [6]   [1] [PPP]
    [NAS-Identifier(32)]           [5]   [Sysname]
    [Acct-Session-Id(44)]          [40]  [00000008201707241008280000000c16100171]
    [CHAP-Challenge(60)]           [18]  [******]
    [NAS-Port-Type(61)]            [6]   [15] [Ethernet]

Received a RADIUS authentication response.
  Server IP    : 192.168.1.110
  Source IP    : 192.168.1.166
  VPN instance : N/A
  Server port  : 1812
  Packet type  : Access-Reject
  Packet length: 20 bytes
  Packet ID    : 0
  Reply-Message: "E63032: Incorrect password. You can retry 9 times."

Sent a RADIUS start-accounting request.
  Server IP    : 192.168.1.110
  Source  IP   : 192.168.1.166
  VPN instance : N/A
  Server port  : 1813
  Packet type  : Start-accounting request
  Packet length: 63 bytes
  Packet ID    : 1
  Attribute list:
    [User-Name(1)]                 [6]   [user1]
    [Acct-Status-Type(40)]         [6]   [1] [Start]
    [NAS-IP-Address(4)]            [6]   [192.168.1.166]
    [NAS-Identifier(32)]           [5]   [Sysname]
    [Acct-Session-Id(44)]          [40]  [00000008201707241008280000000c16100171]

Received a RADIUS start-accounting response.
  Server  IP   : 192.168.1.110
  Source  IP   : 192.168.1.166
  VPN instance : N/A
  Server port  : 1813
  Packet type  : Start-accounting response
  Packet length: 20 bytes
  Packet ID    : 1

Sent a RADIUS stop-accounting request.
  Server  IP   : 192.168.1.110
  Source  IP   : 192.168.1.166
  VPN instance : N/A
  Server port  : 1813
  Packet type  : Stop-accounting request
```

```
  Packet length: 91 bytes
  Packet ID    : 1
  Attribute list:
    [User-Name(1)]                [6]   [user1]
    [Acct-Status-Type(40)]        [6]   [2] [Stop]
    [NAS-IP-Address(4)]           [6]   [192.168.1.166]
    [NAS-Identifier(32)]          [5]   [Sysname]
    [Acct-Delay-Time(41)]         [6]   [0]
    [Acct-Session-Id(44)]         [40]  [00000008201707241008280000000c16100171]
    [Acct-Terminate-Cause(49)]    [6]   [1] [User Request]

Received a RADIUS stop-accounting response.
  Server  IP   : 192.168.1.110
  Source  IP   : 192.168.1.166
  VPN instance : N/A
  Server port  : 1813
  Packet type  : Stop-accounting response
  Packet length: 20 bytes
  Packet ID    : 1

Test result: Failed
```

Perform an AAA test and display brief information about the test. The test uses username **user1**, password **123456** and the CHAP authentication method to test RADIUS server at 192.168.1.110 in RADIUS scheme **test**.

```
<Sysname> test-aaa user user1 password 123456 radius-scheme test radius-server
192.168.1.110 1812
Sent a RADIUS authentication request.
Received a RADIUS authentication response.

Test result: Successful
```

Table 9 Command output

Field	Description
Server IP	IP address of the server.
Source IP	Source IP address of the RADIUS packet.
VPN instance	This field is not supported in the current software version. MPLS L3VPN instance to which the server belongs. This field displays **N/A** if the server belongs to the public network.
Server port	UDP port number of the server.
Packet type	Type of the RADIUS packet: • Authentication request. • Access-Accept. • Access-Reject. • Start-accounting request. • Start-accounting response. • Stop-accounting request. • Stop-accounting response.

Field	Description
Packet length	Total length of the RADIUS packet, in bytes.
Packet ID	ID of the RADIUS packet. This field is used to identity a pair of request and response packets.
[*attribute-name* (*code*)] [*length*] [*value*] [*description*]	Information about a RADIUS attribute: • ***attribute-name***—Name of the attribute. • ***code***—Code of the attribute. • ***length***—Length of the attribute, in bytes. • ***value***—Value of the attribute. • ***description***—Description of the attribute.
Reply-Message:	The RADIUS server rejected the authentication request and replied a message.
Test result	Result of the AAA test: • **Successful**—The test has succeeded. • **Failed**—The test has failed. If any request is rejected, the test fails.

Related commands

`radius scheme`

`radius attribute-test-group`

timer quiet (RADIUS scheme view)

Use **`timer quiet`** to set the quiet timer for the servers specified in a RADIUS scheme.

Use **`undo timer quiet`** to restore the default.

Syntax

`timer quiet` *`minutes`*

`undo timer quiet`

Default

The server quiet timer period is 5 minutes in a RADIUS scheme.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

`minutes`: Specifies the server quiet period in minutes, in the range of 0 to 255. If you set this argument to 0, the device does not change the state of the current server for a user when the server is unreachable. It sends an authentication or accounting request of the user to the next server in active state. For an authentication or accounting request of a new user, it still tries to send the request to the current server because the current server is in active state.

Usage guidelines

Make sure the server quiet timer is set correctly.

A timer that is too short might result in frequent authentication or accounting failures. This is because the device will continue to attempt to communicate with an unreachable server that is in active state.

A timer that is too long might temporarily block a reachable server that has recovered from a failure. This is because the server will remain in blocked state until the timer expires.

Examples

In RADIUS scheme **radius1**, set the quiet timer to 10 minutes for the servers.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] timer quiet 10
```

Related commands

display radius scheme

timer realtime-accounting (RADIUS scheme view)

Use **timer realtime-accounting** to set the real-time accounting interval.

Use **undo timer realtime-accounting** to restore the default.

Syntax

timer realtime-accounting *interval* [**second**]

undo timer realtime-accounting

Default

The real-time accounting interval is 12 minutes.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

interval: Specifies the real-time accounting interval in the range of 0 to 71582.

second: Specifies the measurement unit as second. If you do not specify this keyword, the real-time accounting interval is measured in minutes.

Usage guidelines

When the real-time accounting interval on the device is not zero, the device sends online user accounting information to the RADIUS accounting server at the configured interval.

When the real-time accounting interval on the device is zero, the device sends online user accounting information to the RADIUS accounting server at the real-time accounting interval configured on the server. If the real-time accounting interval is not configured on the server, the device does not send online user accounting information.

A short interval helps improve accounting precision but requires many system resources.

Table 10 Recommended real-time accounting intervals

Number of users	Real-time accounting interval
1 to 99	3 minutes
100 to 499	6 minutes
500 to 999	12 minutes
1000 or more	15 minutes or longer

When you modify the real-time accounting interval, the following rules apply to users that have been online before the modification:

- If you modify the real-time accounting interval from a non-zero value to zero or from zero to a non-zero value, the modification does not take effect on these users. These users still use the old real-time accounting interval.
- If you modify the real-time accounting interval from a non-zero value to another non-zero value, the modification takes effect immediately on these users.

If a user uses RADIUS accounting but not RADIUS authentication and authorization, the device performs real-time accounting for that user only based on the real-time accounting interval set in the user's RADIUS accounting scheme. The real-time accounting interval assigned by the RADIUS accounting server does not take effect.

Examples

In RADIUS scheme **radius1**, set the real-time accounting interval to 51 minutes.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] timer realtime-accounting 51
```

Related commands

retry realtime-accounting

timer response-timeout (RADIUS scheme view)

Use **timer response-timeout** to set the RADIUS server response timeout timer.

Use **undo timer response-timeout** to restore the default.

Syntax

timer response-timeout *seconds*

undo timer response-timeout

Default

The RADIUS server response timeout period is 3 seconds.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

seconds: Specifies the RADIUS server response timeout period, in the range of 1 to 10 seconds.

Usage guidelines

If a NAS receives no response from the RADIUS server in a period of time after sending a RADIUS request, it resends the request so that the user has more opportunity to obtain the RADIUS service. The NAS uses the RADIUS server response timeout timer to control the transmission interval.

If the client times out during the authentication process, the user is immediately logged off. To avoid user logoffs, the value multiplied by the following items cannot be larger than the client timeout period defined by the access module:

- The maximum number of RADIUS packet transmission attempts.
- The RADIUS server response timeout period.
- The number of RADIUS servers in the RADIUS scheme.

When the device sends a RADIUS request to a new RADIUS server, it checks the total amount of time it has taken to transmit the RADIUS packet. If the amount of time has reached 300 seconds, the device stops sending the RADIUS request to the next RADIUS server. As a best practice, consider the number of RADIUS servers when you configure the maximum number of packet transmission attempts and the RADIUS server response timeout period.

Examples

In RADIUS scheme **radius1**, set the RADIUS server response timeout timer to 5 seconds.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] timer response-timeout 5
```

Related commands

display radius scheme

retry

user-name-format (RADIUS scheme view)

Use **user-name-format** to specify the format of the username to be sent to a RADIUS server.

Use **undo user-name-format** to restore the default.

Syntax

user-name-format { **keep-original** | **with-domain** | **without-domain** }

undo user-name-format

Default

The ISP domain name is included in the usernames sent to a RADIUS server.

Views

RADIUS scheme view

Predefined user roles

network-admin

Parameters

keep-original: Sends the username to the RADIUS server as the username is entered.

with-domain: Includes the ISP domain name in the username sent to the RADIUS server.

without-domain: Excludes the ISP domain name from the username sent to the RADIUS server.

Usage guidelines

A username is generally in the *userid@isp-name* format, of which the *isp-name* argument is used by the device to determine the ISP domain to which a user belongs. Some earlier RADIUS servers, however, cannot recognize a username containing an ISP domain name. Before sending a username including a domain name to such a RADIUS server, the device must remove the domain name. This command allows you to specify whether to include a domain name in a username sent to a RADIUS server.

If a RADIUS scheme defines that the username is sent without the ISP domain name, do not apply the scheme to more than one ISP domain. Otherwise, the RADIUS server will consider two users in different ISP domains but with the same *userid* as one user.

For 802.1X users using EAP authentication, the **user-name-format** command configured for a RADIUS scheme does not take effect. The device does not change the usernames from clients before forwarding them to the RADIUS server.

Examples

In RADIUS scheme **radius1**, configure the device to remove the domain name from the usernames sent to the RADIUS servers.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] user-name-format without-domain
```

Related commands

display radius scheme

HWTACACS commands

data-flow-format (HWTACACS scheme view)

Use **data-flow-format** to set the data flow and packet measurement units for traffic statistics.

Use **undo data-flow-format** to restore the default.

Syntax

data-flow-format { **data** { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** } | **packet** { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** } } *

undo data-flow-format { **data** | **packet** }

Default

Traffic is counted in bytes and packets.

Views

HWTACACS scheme view

Predefined user roles

network-admin

Parameters

data: Specifies the unit for data flows.

byte: Specifies the unit as byte.

giga-byte: Specifies the unit as gigabyte.

kilo-byte: Specifies the unit as kilobyte.

mega-byte: Specifies the unit as megabyte.

packet: Specifies the unit for data packets.

giga-packet: Specifies the unit as giga-packet.

kilo-packet: Specifies the unit as kilo-packet.

mega-packet: Specifies the unit as mega-packet.

one-packet: Specifies the unit as one-packet.

Usage guidelines

The data flow and packet measurement units for traffic statistics must be the same as configured on the HWTACACS accounting servers. Otherwise, accounting results might be incorrect.

Examples

In HWTACACS scheme **hwt1**, set the data flow and packet measurement units for traffic statistics to kilobyte and kilo-packet, respectively.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] data-flow-format data kilo-byte packet kilo-packet
```

Related commands

display hwtacacs scheme

display hwtacacs scheme

Use **display hwtacacs scheme** to display the configuration or statistics of HWTACACS schemes.

Syntax

display hwtacacs scheme [*hwtacacs-scheme-name* [**statistics**]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

hwtacacs-scheme-name: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters. If you do not specify an HWTACACS scheme, this command displays the configuration of all HWTACACS schemes.

statistics: Displays the HWTACACS service statistics. If you do not specify this keyword, the command displays the configuration of the specified HWTACACS scheme.

Examples

Displays the configuration of all HWTACACS schemes.

```
<Sysname> display hwtacacs scheme
Total 1 HWTACACS schemes


------------------------------------------------------------------------
HWTACACS Scheme Name  : hwtac
  Index : 0
  Primary Auth Server:
    Host name: Not configured
    IP  : 2.2.2.2         Port: 49     State: Active
    VPN Instance: Not configured
    Single-connection: Enabled
  Primary Author Server:
    Host name: Not configured
    IP  : 2.2.2.2         Port: 49     State: Active
    VPN Instance: Not configured
    Single-connection: Disabled
  Primary Acct Server:
```

```
    Host name: Not configured
    IP  : Not Configured  Port: 49     State: Block
    VPN Instance: Not configured
    Single-connection: Disabled

  VPN Instance                          : Not configured
  NAS IP Address                        : 2.2.2.3
  Server Quiet Period(minutes)          : 5
  Realtime Accounting Interval(minutes) : 12
  Stop-accounting packets buffering     : Enabled
    Retransmission times                : 100
  Response Timeout Interval(seconds)    : 5
  Username Format                       : with-domain
  Data flow unit                        : Byte
  Packet unit                           : one
------------------------------------------------------------------
```

Table 11 Command output

Field	Description
Index	Index number of the HWTACACS scheme.
Primary Auth Server	Primary HWTACACS authentication server.
Primary Author Server	Primary HWTACACS authorization server.
Primary Acct Server	Primary HWTACACS accounting server.
Secondary Auth Server	Secondary HWTACACS authentication server.
Secondary Author Server	Secondary HWTACACS authorization server.
Secondary Acct Server	Secondary HWTACACS accounting server.
Host name	Host name of the server. This field displays **Not configured** in the following situations: • The server is not configured. • The server is specified by IP address.
IP	IP address of the server. This field displays **Not configured** in the following situations: • The server is not configured. • The server is specified by hostname, and the hostname is not resolved.
Port	Service port of the HWTACACS server. If no port configuration is performed, this field displays the default port number.
State	Status of the HWTACACS server: active or blocked.
VPN Instance	This field is not supported in the current software version. MPLS L3VPN instance to which the HWTACACS server or scheme belongs. If no VPN instance is specified for the server or scheme, this field displays **Not configured**.
Single-connection	Single connection status: • **Enabled**—Establish only one TCP connection for all users to communicate with the server. • **Disabled**—Establish a TCP connection for each user to

Field	Description
	communicate with the server.
NAS IP Address	Source interface or source IP addresses for outgoing HWTACACS packets. This field displays **Not configured** if no source interface or source IP addresses are specified for outgoing HWTACACS packets.
Server Quiet Period(minutes)	Quiet period for the primary servers, in minutes.
Realtime Accounting Interval(minutes)	Real-time accounting interval, in minutes.
Stop-accounting packets buffering	Whether buffering of nonresponded HWTACACS stop-accounting requests is enabled.
Retransmission times	Maximum number of transmission attempts for individual HWTACACS stop-accounting requests.
Response Timeout Interval(seconds)	HWTACACS server response timeout period, in seconds.
Username Format	Format for the usernames sent to the HWTACACS server: • **with-domain**—Includes the domain name. • **without-domain**—Excludes the domain name. • **keep-original**—Forwards the username as the username is entered.
Data flow unit	Measurement unit for data flows.
Packet unit	Measurement unit for packets.

Display statistics for HWTACACS scheme **tac**.

```
<Sysname> display hwtacacs scheme tac statistics

Primary authentication server : 111.8.0.244
    Round trip time:                                20 seconds
    Request packets:                                1
    Login request packets:                          1
    Change-password request packets:                0
    Request packets including plaintext passwords:  0
    Request packets including ciphertext passwords: 0
    Response packets:                               2
    Pass response packets:                          1
    Failure response packets:                       0
    Get-data response packets:                      0
    Get-username response packets:                  0
    Get-password response packets:                  1
    Restart response packets:                       0
    Error response packets:                         0
    Follow response packets:                        0
    Malformed response packets:                     0
    Continue packets:                               1
    Continue-abort packets:                         0
    Pending request packets:                        0
    Timeout packets:                                0
    Unknown type response packets:                  0
```

```
    Dropped response packets:                      0

Primary authorization server :111.8.0.244
    Round trip time:                               1 seconds
    Request packets:                               1
    Response packets:                              1
    PassAdd response packets:                      1
    PassReply response packets:                    0
    Failure response packets:                      0
    Error response packets:                        0
    Follow response packets:                       0
    Malformed response packets:                    0
    Pending request packets:                       0
    Timeout packets:                               0
    Unknown type response packets:                 0
    Dropped response packets:                      0

Primary accounting server :111.8.0.244
    Round trip time:                               0 seconds
    Request packets:                               2
    Accounting start request packets:              1
    Accounting stop request packets:               1
    Accounting update request packets:             0
    Pending request packets:                       0
    Response packets:                              2
    Success response packets:                      2
    Error response packets:                        0
    Follow response packets:                       0
    Malformed response packets:                    0
    Timeout response packets:                      0
    Unknown type response packets:                 0
    Dropped response packets:                      0
```

Table 12 Command output

Field	Description
Primary authentication server	Primary HWTACACS authentication server.
Primary authorization server	Primary HWTACACS authorization server.
Primary accounting server	Primary HWTACACS accounting server.
Secondary authentication server	Secondary HWTACACS authentication server.
Secondary authorization server	Secondary HWTACACS authorization server.
Secondary accounting server	Secondary HWTACACS accounting server.
Round trip time	The time interval during which the device processed a pair of request and response. The unit is second.
Request packets	Total number of sent request packets.
Login request packets	Number of sent login request packets.
Change-password request packets	Number of sent request packets for changing passwords.

Field	Description
Request packets including plaintext passwords	Number of request packets that include plaintext passwords.
Request packets including ciphertext passwords	Number of request packets that include ciphertext passwords.
Response packets	Total number of received response packets.
Pass response packets	Number of response packets indicating successful authentication.
Failure response packets	Number of response packets indicating authentication or authorization failure.
Get-data response packets	Number of response packets for obtaining user data.
Get-username response packets	Number of response packets for obtaining usernames.
Get-password response packets	Number of response packets for obtaining passwords.
Restart response packets	Number of response packets for reauthentication.
Error response packets	Number of error-type response packets.
Follow response packets	Number of follow-type response packets.
Malformed response packets	Number of malformed response packets.
Continue packets	Number of sent Continue packets.
Continue-abort packets	Number of sent Continue-abort packets.
Pending request packets	Number of request packets waiting for a response.
Timeout packets/Timeout response packets	Number of timeout response packets.
Unknown type response packets	Number of unknown-type response packets.
Dropped response packets	Number of dropped response packets.
PassAdd response packets	Number of received PassAdd response packets. The packets indicate that all requested authorization attributes are assigned and additional authorization attributes are added.
PassReply response packets	Number of received PassReply response packets. The device uses the specified authorization attributes in the packets to replace the requested authorization attributes.
Accounting start request packets	Number of accounting start request packets.
Accounting stop request packets	Number of accounting stop request packets.
Accounting update request packets	Number of accounting update request packets.
Success response packets	Number of accounting success response packets.

Related commands

`reset hwtacacs statistics`

display stop-accounting-buffer (for HWTACACS)

Use **`display stop-accounting-buffer`** to display information about buffered HWTACACS stop-accounting requests to which no responses have been received.

Syntax

`display stop-accounting-buffer hwtacacs-scheme` *`hwtacacs-scheme-name`*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

Examples

Display information about nonresponded stop-accounting requests buffered for HWTACACS scheme hwt1.

```
<Sysname> display stop-accounting-buffer hwtacacs-scheme hwt1
Total entries: 2
Scheme    IP address        Username      First sending time     Attempts
hwt1      192.168.100.1     abc           23:27:16-08/31/2015    19
hwt1      192.168.90.6      bob           23:33:01-08/31/2015    20
```

Table 13 Command output

Field	Description
First sending time	Time when the stop-accounting request was first sent.
Attempts	Number of attempts that were made to send the stop-accounting request.

Related commands

reset stop-accounting-buffer (for HWTACACS)

retry stop-accounting (HWTACACS scheme view)

stop-accounting-buffer enable (HWTACACS scheme view)

user-name-format (HWTACACS scheme view)

hwtacacs nas-ip

Use **hwtacacs nas-ip** to specify a source interface or source IP address for outgoing HWTACACS packets.

Use **undo hwtacacs nas-ip** to delete the specified source interface or source IP address for outgoing HWTACACS packets.

Syntax

hwtacacs nas-ip { **interface** *interface-type interface-number* | { *ipv4-address* | **ipv6** *ipv6-address* } }

undo hwtacacs nas-ip { **interface** | { *ipv4-address* | **ipv6** *ipv6-address* } }

Default

The source IP address of an HWTACACS packet sent to the server is the primary IPv4 address or the IPv6 address of the outbound interface.

Views

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a source interface by its type and number. The device uses the primary IPv4 address or the IPv6 address of the interface as the source IP address of an outgoing HWTACACS packet.

ipv4-address: Specifies an IPv4 address, which must be an address of the device. The IP address cannot be 0.0.0.0, 255.255.255.255, a class D address, a class E address, or a loopback address.

ipv6 *ipv6-address*: Specifies an IPv6 address, which must be a unicast address of the device and cannot be a loopback address or a link-local address.

Usage guidelines

The source IP address of HWTACACS packets that a NAS sends must match the IP address of the NAS that is configured on the HWTACACS server. An HWTACACS server identifies a NAS by IP address. Upon receiving an HWTACACS packet, the HWTACACS server checks the source IP address of the packet.

- If the source IP address of the packet is the IP address of a managed NAS, the server processes the packet.
- If the source IP address of the packet is not the IP address of a managed NAS, the server drops the packet.

As a best practice, specify a loopback interface address as the source IP address for outgoing HWTACACS packets to avoid HWTACACS packet loss caused by physical port errors.

If you use both the **nas-ip** command and **hwtacacs nas-ip** command, the following guidelines apply:

- The setting configured by using the **nas-ip** command in HWTACACS scheme view applies only to the HWTACACS scheme.
- The setting configured by using the **hwtacacs nas-ip** command in system view applies to all HWTACACS schemes.
- The setting in HWTACACS scheme view takes precedence over the setting in system view.

You can specify only one source IPv4 address and one source IPv6 address in system view.

You can specify only one source interface to provide the source IP address for outgoing HWTACACS packets. Make sure the route between the source interface and the HWTACACS server is reachable.

The source interface configuration and the source IP address configuration overwrite each other.

Examples

Specify IP address 129.10.10.1 as the source IP address for HWTACACS packets.

```
<Sysname> system-view
[Sysname] hwtacacs nas-ip 129.10.10.1
```

Related commands

nas-ip (HWTACACS scheme view)

hwtacacs scheme

Use **hwtacacs scheme** to create an HWTACACS scheme and enter its view, or enter the view of an existing HWTACACS scheme.

Use **undo hwtacacs scheme** to delete an HWTACACS scheme.

Syntax

hwtacacs scheme *hwtacacs-scheme-name*

undo hwtacacs scheme *hwtacacs-scheme-name*

Default

No HWTACACS schemes exist.

Views

System view

Predefined user roles

network-admin

Parameters

hwtacacs-scheme-name: Specifies the HWTACACS scheme name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

An HWTACACS scheme can be used by more than one ISP domain at the same time.

You can configure a maximum of 16 HWTACACS schemes.

Examples

Create an HWTACACS scheme named **hwt1** and enter HWTACACS scheme view.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1]
```

Related commands

display hwtacacs scheme

key (HWTACACS scheme view)

Use **key** to set the shared key for secure HWTACACS authentication, authorization, or accounting communication.

Use **undo key** to delete the shared key for secure HWTACACS authentication, authorization, or accounting communication.

Syntax

key { **accounting** | **authentication** | **authorization** } { **cipher** | **simple** } *string*

undo key { **accounting** | **authentication** | **authorization** }

Default

No shared key is configured for secure HWTACACS authentication, authorization, or accounting communication.

Views

HWTACACS scheme view

Predefined user roles

network-admin

Parameters

accounting: Specifies the shared key for secure HWTACACS accounting communication.

authentication: Specifies the shared key for secure HWTACACS authentication communication.

authorization: Specifies the shared key for secure HWTACACS authorization communication.

cipher: Specifies the key in encrypted form.

simple: Specifies the key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive. In non-FIPS mode, the encrypted form of the key is a string of 1 to 373 characters. The plaintext form of the key is a string of 1 to 255 characters. In FIPS mode, the encrypted form of the key is a string of 15 to 373 characters. The plaintext form of the key is a string of 15 to 255 characters. The plaintext string must contain digits, uppercase letters, lowercase letters, and special characters.

Usage guidelines

The shared keys configured on the device must match those configured on the HWTACACS servers.

Examples

In HWTACACS scheme **hwt1**, set the shared key to **123456TESTauth&!** in plaintext form for secure HWTACACS authentication communication.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] key authentication simple 123456TESTauth&!
```

Set the shared key to **123456TESTautr&!** in plaintext form for secure HWTACACS authorization communication.

```
[Sysname-hwtacacs-hwt1] key authorization simple 123456TESTautr&!
```

Set the shared key to **123456TESTacct&!** in plaintext form for secure HWTACACS accounting communication.

```
[Sysname-hwtacacs-hwt1] key accounting simple 123456TESTacct&!
```

Related commands

display hwtacacs scheme

nas-ip (HWTACACS scheme view)

Use **nas-ip** to specify a source interface or source IP address for outgoing HWTACACS packets.

Use **undo nas-ip** to delete the specified source interface or source IP address for outgoing HWTACACS packets.

Syntax

nas-ip { *ipv4-address* | **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }

undo nas-ip [**interface** | **ipv6**]

Default

The source IP address of an outgoing HWTACACS packet is that configured by using the **hwtacacs nas-ip** command in system view.

If the **hwtacacs nas-ip** command is not used, the source IP address is the primary IP address of the outbound interface.

Views

HWTACACS scheme view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a source interface by its type and number. The device uses the primary IPv4 address or the IPv6 address of the interface as the source IP address of an outgoing HWTACACS packet.

ipv4-address: Specifies an IPv4 address, which must be an address of the device. The IP address cannot be 0.0.0.0, 255.255.255.255, a class D address, a class E address, or a loopback address.

ipv6 *ipv6-address*: Specifies an IPv6 address, which must be a unicast address of the device and cannot be a loopback address or a link-local address.

Usage guidelines

The source IP address of HWTACACS packets that a NAS sends must match the IP address of the NAS that is configured on the HWTACACS server. An HWTACACS server identifies a NAS by IP address. Upon receiving an HWTACACS packet, the HWTACACS server checks the source IP address of the packet.

- If the source IP address of the packet is the IP address of a managed NAS, the server processes the packet.
- If the source IP address of the packet is not the IP address of a managed NAS, the server drops the packet.

As a best practice, specify a loopback interface address as the source IP address for outgoing HWTACACS packets to avoid HWTACACS packet loss caused by physical port errors.

If you use both the **nas-ip** command and **hwtacacs nas-ip** command, the following guidelines apply:

- The setting configured by using the **nas-ip** command in HWTACACS scheme view applies only to the HWTACACS scheme.
- The setting configured by using the **hwtacacs nas-ip** command in system view applies to all HWTACACS schemes.
- The setting in HWTACACS scheme view takes precedence over the setting in system view.

For an HWTACACS scheme, the following restrictions apply:

- You can specify only one source IPv4 address and one source IPv6 address for outgoing HWTACACS packets.
- You can specify only one source interface to provide the source IP address for outgoing HWTACACS packets. Make sure the route between the source interface and the HWTACACS server is reachable.
- The source interface configuration and the source IP address configuration overwrite each other.

If you do not specify any parameter for the **undo nas-ip** command, the command deletes the configured source IPv4 address for outgoing HWTACACS packets.

Examples

In HWTACACS scheme **hwt1**, specify IP address 10.1.1.1 as the source address for outgoing HWTACACS packets.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] nas-ip 10.1.1.1
```

Related commands

display hwtacacs scheme

hwtacacs nas-ip

primary accounting (HWTACACS scheme view)

Use **primary accounting** to specify the primary HWTACACS accounting server.

Use **undo primary accounting** to restore the default.

Syntax

primary accounting { *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **single-connection**] *

undo primary accounting

Default

The primary HWTACACS accounting server is not specified.

Views

HWTACACS scheme view

Predefined user roles

network-admin

Parameters

host-name: Specifies the host name of the primary HWTACACS accounting server, a case-insensitive string of 1 to 253 characters.

ipv4-address: Specifies an IPv4 address of the primary HWTACACS accounting server.

ipv6 *ipv6-address*: Specifies an IPv6 address of the primary HWTACACS accounting server.

port-number: Specifies the service port number of the primary HWTACACS accounting server. The value range for the TCP port number is 1 to 65535. The default setting is 49.

key: Specifies the shared key for secure communication with the primary HWTACACS accounting server.

cipher: Specifies the key in encrypted form.

simple: Specifies the key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive. In non-FIPS mode, the encrypted form of the key is a string of 1 to 373 characters. The plaintext form of the key is a string of 1 to 255 characters. In FIPS mode, the encrypted form of the key is a string of 15 to 373 characters. The plaintext form of the key is a string of 15 to 255 characters. The plaintext string must contain digits, uppercase letters, lowercase letters, and special characters.

single-connection: The device and the primary HWTACACS accounting server use the same TCP connection to exchange accounting packets for all users. If you do not specify this keyword, the

device establishes a new TCP connection each time it exchanges accounting packets with the primary accounting server for a user.

Usage guidelines

Make sure the port number and shared key settings of the primary HWTACACS accounting server are the same as those configured on the server.

Two accounting servers specified for a scheme, primary or secondary, cannot have identical host name, IP address, and port number settings.

As a best practice, specify the **single-connection** keyword to reduce TCP connections for improving system performance if the HWTACACS server supports the single-connection method.

You can remove an accounting server only when it is not used for user accounting. Removing an accounting server affects only accounting processes that occur after the remove operation.

Examples

In HWTACACS scheme **hwt1**, specify the primary accounting server with IP address 10.163.155.12, TCP port number 49, and plaintext shared key **123456TESTacct&!**.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] primary accounting 10.163.155.12 49 key simple 123456TESTacct&!
```

Related commands

display hwtacacs scheme

key (HWTACACS scheme view)

secondary accounting (HWTACACS scheme view)

primary authentication (HWTACACS scheme view)

Use **primary authentication** to specify the primary HWTACACS authentication server.

Use **undo primary authentication** to restore the default.

Syntax

primary authentication { *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **single-connection**] *

undo primary authentication

Default

The primary HWTACACS authentication server is not specified.

Views

HWTACACS scheme view

Predefined user roles

network-admin

Parameters

host-name: Specifies the host name of the primary HWTACACS authentication server, a case-insensitive string of 1 to 253 characters.

ipv4-address: Specifies the IPv4 address of the primary HWTACACS authentication server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the primary HWTACACS authentication server.

port-number: Specifies the service port number of the primary HWTACACS authentication server. The value range for the TCP port number is 1 to 65535. The default setting is 49.

key: Specifies the shared key for secure communication with the primary HWTACACS authentication server.

cipher: Specifies the key in encrypted form.

simple: Specifies the key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive. In non-FIPS mode, the encrypted form of the key is a string of 1 to 373 characters. The plaintext form of the key is a string of 1 to 255 characters. In FIPS mode, the encrypted form of the key is a string of 15 to 373 characters. The plaintext form of the key is a string of 15 to 255 characters. The plaintext string must contain digits, uppercase letters, lowercase letters, and special characters.

single-connection: The device and the primary HWTACACS authentication server use the same TCP connection to exchange all authentication packets for all users. If you do not specify this keyword, the device establishes a new TCP connection each time it exchanges authentication packets with the primary authentication server for a user.

Usage guidelines

Make sure the port number and shared key settings of the primary HWTACACS authentication server are the same as those configured on the server.

Two authentication servers specified for a scheme, primary or secondary, cannot have identical host name, IP address, and port number settings.

As a best practice, specify the **single-connection** keyword to reduce TCP connections for improving system performance if the HWTACACS server supports the single-connection method.

You can remove an authentication server only when it is not used for user authentication. Removing an authentication server affects only authentication processes that occur after the remove operation.

Examples

In HWTACACS scheme **hwt1**, specify the primary authentication server with IP address 10.163.155.13, TCP port number 49, and plaintext shared key **123456TESTauth&!**.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] primary authentication 10.163.155.13 49 key simple
123456TESTauth&!
```

Related commands

display hwtacacs scheme

key (HWTACACS scheme view)

secondary authentication (HWTACACS scheme view)

primary authorization

Use **primary authorization** to specify the primary HWTACACS authorization server.

Use **undo primary authorization** to restore the default.

Syntax

primary authorization { *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **single-connection**] *

undo primary authorization

Default

The primary HWTACACS authorization server is not specified.

Views

HWTACACS scheme view

Predefined user roles

network-admin

Parameters

host-name: Specifies the host name of the primary HWTACACS authorization server, a case-insensitive string of 1 to 253 characters.

ipv4-address: Specifies the IPv4 address of the primary HWTACACS authorization server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the primary HWTACACS authorization server.

port-number: Specifies the service port number of the primary HWTACACS authorization server. The value range for the TCP port number is 1 to 65535. The default setting is 49.

key: Specifies the shared key for secure communication with the primary HWTACACS authorization server.

cipher: Specifies the key in encrypted form.

simple: Specifies the key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive. In non-FIPS mode, the encrypted form of the key is a string of 1 to 373 characters. The plaintext form of the key is a string of 1 to 255 characters. In FIPS mode, the encrypted form of the key is a string of 15 to 373 characters. The plaintext form of the key is a string of 15 to 255 characters. The plaintext string must contain digits, uppercase letters, lowercase letters, and special characters.

single-connection: The device and the primary HWTACACS authorization server use the same TCP connection to exchange all authorization packets for all users. If you do not specify this keyword, the device establishes a new TCP connection each time it exchanges authorization packets with the primary authorization server for a user.

Usage guidelines

Make sure the port number and shared key settings of the primary HWTACACS authorization server are the same as those configured on the server.

Two authorization servers specified for a scheme, primary or secondary, cannot have identical host name, IP address, and port number settings.

As a best practice, specify the **single-connection** keyword to reduce TCP connections for improving system performance if the HWTACACS server supports the single-connection method.

You can remove an authorization server only when it is not used for user authorization. Removing an authorization server affects only authorization processes that occur after the remove operation.

Examples

In HWTACACS scheme **hwt1**, specify the primary authorization server with IP address 10.163.155.13, TCP port number 49, and plaintext shared key **123456TESTautr&!**.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] primary authorization 10.163.155.13 49 key simple
123456TESTautr&!
```

Related commands

display hwtacacs scheme

key (HWTACACS scheme view)

secondary authorization (HWTACACS scheme view)

reset hwtacacs statistics

Use **reset hwtacacs statistics** to clear HWTACACS statistics.

Syntax

reset hwtacacs statistics { **accounting** | **all** | **authentication** | **authorization** }

Views

User view

Predefined user roles

network-admin

Parameters

accounting: Clears the HWTACACS accounting statistics.

all: Clears all HWTACACS statistics.

authentication: Clears the HWTACACS authentication statistics.

authorization: Clears the HWTACACS authorization statistics.

Examples

Clear all HWTACACS statistics.

```
<Sysname> reset hwtacacs statistics all
```

Related commands

display hwtacacs scheme

reset stop-accounting-buffer (for HWTACACS)

Use **reset stop-accounting-buffer** to clear buffered HWTACACS stop-accounting requests to which no responses have been received.

Syntax

reset stop-accounting-buffer hwtacacs-scheme *hwtacacs-scheme-name*

Views

User view

Predefined user roles

network-admin

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

Examples

Clear nonresponded stop-accounting requests buffered for HWTACACS scheme hwt1.

```
<Sysname> reset stop-accounting-buffer hwtacacs-scheme hwt1
```

Related commands

display stop-accounting-buffer (for HWTACACS)

stop-accounting-buffer enable (HWTACACS scheme view)

retry stop-accounting (HWTACACS scheme view)

Use **retry stop-accounting** to set the maximum number of transmission attempts for individual HWTACACS stop-accounting requests.

Use **undo retry stop-accounting** to restore the default.

Syntax

retry stop-accounting *retries*

undo retry stop-accounting

Default

The maximum number of transmission attempts for individual HWTACACS stop-accounting requests is 100.

Views

HWTACACS scheme view

Predefined user roles

network-admin

Parameters

retries: Specifies the maximum number of transmission attempts for HWTACACS stop-accounting requests. The value range is 1 to 300.

Examples

In HWTACACS scheme **hwt1**, set the maximum number of HWTACACS stop-accounting attempts to 300.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] retry stop-accounting 300
```

Related commands

display stop-accounting-buffer (for HWTACACS)

timer response-timeout (HWTACACS scheme view)

secondary accounting (HWTACACS scheme view)

Use **secondary accounting** to specify a secondary HWTACACS accounting server.

Use **undo secondary accounting** to remove a secondary HWTACACS accounting server.

Syntax

secondary accounting { *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **single-connection**] *

undo secondary accounting [{ *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number*]]

Default

No secondary HWTACACS accounting servers are specified.

Views

HWTACACS scheme view

Predefined user roles

network-admin

Parameters

host-name: Specifies the host name of a secondary HWTACACS accounting server, a case-insensitive string of 1 to 253 characters.

ipv4-address: Specifies the IPv4 address of a secondary HWTACACS accounting server.

ipv6 *ipv6-address*: Specifies the IPv6 address of a secondary HWTACACS accounting server.

port-number: Specifies the service port number of the secondary HWTACACS accounting server. The value range for the TCP port number is 1 to 65535. The default setting is 49.

key: Specifies the shared key for secure communication with the secondary HWTACACS accounting server.

cipher: Specifies the key in encrypted form.

simple: Specifies the key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive. In non-FIPS mode, the encrypted form of the key is a string of 1 to 373 characters. The plaintext form of the key is a string of 1 to 255 characters. In FIPS mode, the encrypted form of the key is a string of 15 to 373 characters. The plaintext form of the key is a string of 15 to 255 characters. The plaintext string must contain digits, uppercase letters, lowercase letters, and special characters.

single-connection: The device and the secondary HWTACACS accounting server use the same TCP connection to exchange all accounting packets for all users. If you do not specify this keyword, the device establishes a new TCP connection each time it exchanges accounting packets with the secondary accounting server for a user.

Usage guidelines

Make sure the port number and shared key settings of the secondary HWTACACS accounting server are the same as those configured on the server.

An HWTACACS scheme supports a maximum of 16 secondary HWTACACS accounting servers. If the primary server fails, the device tries to communicate with a secondary server in active state. The device connects to the secondary servers in the order they are configured.

If you do not specify any parameters for the **undo secondary accounting** command, the command removes all secondary accounting servers.

Two accounting servers specified for a scheme, primary or secondary, cannot have identical host name, IP address, and port number settings.

As a best practice, specify the **single-connection** keyword to reduce TCP connections for improving system performance if the HWTACACS server supports the single-connection method.

You can remove an accounting server only when it is not used for user accounting. Removing an accounting server affects only accounting processes that occur after the remove operation.

Examples

In HWTACACS scheme **hwt1**, specify a secondary accounting server with IP address 10.163.155.12, TCP port number 49, and plaintext shared key **123456TESTacct&!**.

```
<Sysname> system-view
```

```
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] secondary accounting 10.163.155.12 49 key simple 123456TESTacct&!
```

Related commands

display hwtacacs scheme

key (HWTACACS scheme view)

primary accounting (HWTACACS scheme view)

secondary authentication (HWTACACS scheme view)

Use **secondary authentication** to specify a secondary HWTACACS authentication server.

Use **undo secondary authentication** to remove a secondary HWTACACS authentication server.

Syntax

secondary authentication { *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **single-connection**] *

undo secondary authentication [{ *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number*]]

Default

No secondary HWTACACS authentication servers are specified.

Views

HWTACACS scheme view

Predefined user roles

network-admin

Parameters

host-name: Specifies the host name of a secondary HWTACACS authentication server, a case-insensitive string of 1 to 253 characters.

ipv4-address: Specifies the IPv4 address of a secondary HWTACACS authentication server.

ipv6 *ipv6-address*: Specifies the IPv6 address of a secondary HWTACACS authentication server.

port-number: Specifies the service port number of the secondary HWTACACS authentication server. The value range for the TCP port number is 1 to 65535. The default setting is 49.

key: Specifies the shared key for secure communication with the secondary HWTACACS authentication server.

cipher: Specifies the key in encrypted form.

simple: Specifies the key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive. In non-FIPS mode, the encrypted form of the key is a string of 1 to 373 characters. The plaintext form of the key is a string of 1 to 255 characters. In FIPS mode, the encrypted form of the key is a string of 15 to 373 characters. The plaintext form of the key is a string of 15 to 255 characters. The plaintext string must contain digits, uppercase letters, lowercase letters, and special characters.

single-connection: The device and the secondary HWTACACS authentication server use the same TCP connection to exchange all authentication packets for all users. If you do not specify this

keyword, the device establishes a new TCP connection each time it exchanges authentication packets with the secondary authentication server for a user.

Usage guidelines

Make sure the port number and shared key settings of each secondary HWTACACS authentication server are the same as those configured on the corresponding server.

An HWTACACS scheme supports a maximum of 16 secondary HWTACACS authentication servers. If the primary server fails, the device tries to communicate with a secondary server in active state. The device connects to the secondary servers in the order they are configured.

If you do not specify any parameters for the **undo secondary authentication** command, the command removes all secondary authentication servers.

Two authentication servers specified for a scheme, primary or secondary, cannot have identical host name, IP address, and port number settings.

As a best practice, specify the **single-connection** keyword to reduce TCP connections for improving system performance if the HWTACACS server supports the single-connection method.

You can remove an authentication server only when it is not used for user authentication. Removing an authentication server affects only authentication processes that occur after the remove operation.

Examples

In HWTACACS scheme **hwt1**, specify a secondary authentication server with IP address 10.163.155.13, TCP port number 49, and plaintext shared key **123456TESTauth&!**.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] secondary authentication 10.163.155.13 49 key simple
123456TESTauth&!
```

Related commands

display hwtacacs scheme

key (HWTACACS scheme view)

primary authentication (HWTACACS scheme view)

secondary authorization

Use **secondary authorization** to specify a secondary HWTACACS authorization server.

Use **undo secondary authorization** to remove a secondary HWTACACS authorization server.

Syntax

secondary authorization { *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **single-connection**] *

undo secondary authorization [{ *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number*]]

Default

No secondary HWTACACS authorization servers are specified.

Views

HWTACACS scheme view

Predefined user roles

network-admin

Parameters

host-name: Specifies the host name of a secondary HWTACACS authorization server, a case-insensitive string of 1 to 253 characters.

ipv4-address: Specifies the IPv4 address of a secondary HWTACACS authorization server.

ipv6 *ipv6-address*: Specifies the IPv6 address of a secondary HWTACACS authorization server.

port-number: Specifies the service port number of the secondary HWTACACS authorization server. The value range for the TCP port number is 1 to 65535. The default setting is 49.

key: Specifies the shared key for secure communication with the secondary HWTACACS authorization server.

cipher: Specifies the key in encrypted form.

simple: Specifies the key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. This argument is case sensitive. In non-FIPS mode, the encrypted form of the key is a string of 1 to 373 characters. The plaintext form of the key is a string of 1 to 255 characters. In FIPS mode, the encrypted form of the key is a string of 15 to 373 characters. The plaintext form of the key is a string of 15 to 255 characters. The plaintext string must contain digits, uppercase letters, lowercase letters, and special characters.

single-connection: The device and the secondary HWTACACS authorization server use the same TCP connection to exchange all authorization packets for all users. If you do not specify this keyword, the device establishes a new TCP connection each time it exchanges authorization packets with the secondary authorization server for a user.

Usage guidelines

Make sure the port number and shared key settings of the secondary HWTACACS authorization server are the same as those configured on the server.

An HWTACACS scheme supports a maximum of 16 secondary HWTACACS authorization servers. If the primary server fails, the device tries to communicate with a secondary server in active state. The device connects to the secondary servers in the order they are configured.

If you do not specify any parameters for the **undo secondary authorization** command, the command removes all secondary authorization servers.

Two authorization servers specified for a scheme, primary or secondary, cannot have identical host name, IP address, and port number settings.

As a best practice, specify the **single-connection** keyword to reduce TCP connections for improving system performance if the HWTACACS server supports the single-connection method.

You can remove an authorization server only when it is not used for user authorization. Removing an authorization server affects only authorization processes that occur after the remove operation.

Examples

In HWTACACS scheme **hwt1**, specify a secondary authorization server with IP address 10.163.155.13, TCP port number 49, and plaintext shared key **123456TESTautr&!**.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] secondary authorization 10.163.155.13 49 key simple
123456TESTautr&!
```

Related commands

display hwtacacs scheme

key (HWTACACS scheme view)

primary authorization (HWTACACS scheme view)

stop-accounting-buffer enable (HWTACACS scheme view)

Use **stop-accounting-buffer enable** to enable buffering of HWTACACS stop-accounting requests to which no responses have been received.

Use **undo stop-accounting-buffer enable** to disable buffering of HWTACACS stop-accounting requests to which no responses have been received.

Syntax

stop-accounting-buffer enable

undo stop-accounting-buffer enable

Default

The device buffers HWTACACS stop-accounting requests to which no responses have been received.

Views

HWTACACS scheme view

Predefined user roles

network-admin

Usage guidelines

This command enables the device to buffer an HWTACACS stop-accounting request to which no response has been received. The device resends the buffered request until it receives a server response or when the number of transmission attempts reaches the maximum (set by using the **retry stop-accounting** command). If no more attempts are available, the device discards the request. However, if you have removed an accounting server, stop-accounting requests destined for the server are not buffered.

Examples

Enable buffering of HWTACACS stop-accounting requests to which no responses have been received.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] stop-accounting-buffer enable
```

Related commands

display stop-accounting-buffer (for HWTACACS)

reset stop-accounting-buffer (for HWTACACS)

timer quiet (HWTACACS scheme view)

Use **timer quiet** to set the quiet timer for the servers specified in an HWTACACS scheme.

Use **undo timer quiet** to restore the default.

Syntax

timer quiet *minutes*

undo timer quiet

Default

The server quiet period is 5 minutes.

Views

HWTACACS scheme view

Predefined user roles

network-admin

Parameters

minutes: Specifies the server quiet period in minutes, in the range of 1 to 255.

Examples

In HWTACACS scheme **hwt1**, set the server quiet timer to 10 minutes.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] timer quiet 10
```

Related commands

display hwtacacs scheme

timer realtime-accounting (HWTACACS scheme view)

Use **timer realtime-accounting** to set the real-time accounting interval.

Use **undo timer realtime-accounting** to restore the default.

Syntax

timer realtime-accounting *minutes*

undo timer realtime-accounting

Default

The real-time accounting interval is 12 minutes.

Views

HWTACACS scheme view

Predefined user roles

network-admin

Parameters

minutes: Specifies the real-time accounting interval in minutes, in the range of 0 to 60. Setting this interval to 0 disables the device from sending online user accounting information to the HWTACACS accounting server.

Usage guidelines

For real-time accounting, a NAS must transmit the accounting information of online users to the HWTACACS accounting server periodically. This command is used to set the interval.

A short interval helps improve accounting precision but requires many system resources.

Table 14 Recommended real-time accounting intervals

Number of users	Real-time accounting interval
1 to 99	3 minutes

Number of users	Real-time accounting interval
100 to 499	6 minutes
500 to 999	12 minutes
1000 or more	15 minutes or longer

When you modify the real-time accounting interval, the following rules apply to users that have been online before the modification:

- If you modify the real-time accounting interval from a non-zero value to zero or from zero to a non-zero value, the modification does not take effect on these users. These users still use the old real-time accounting interval.
- If you modify the real-time accounting interval from a non-zero value to another non-zero value, the modification takes effect immediately on these users.

Examples

In HWTACACS scheme **hwt1**, set the real-time accounting interval to 51 minutes.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] timer realtime-accounting 51
```

Related commands

display hwtacacs scheme

timer response-timeout (HWTACACS scheme view)

Use **timer response-timeout** to set the HWTACACS server response timeout timer.

Use **undo timer response-timeout** to restore the default.

Syntax

timer response-timeout *seconds*

undo timer response-timeout

Default

The HWTACACS server response timeout time is 5 seconds.

Views

HWTACACS scheme view

Predefined user roles

network-admin

Parameters

seconds: Specifies the HWTACACS server response timeout time, in the range of 1 to 300 seconds.

Usage guidelines

HWTACACS is based on TCP. When the server response timeout timer or the TCP timeout timer times out, the device is disconnected from the HWTACACS server.

The client timeout period of the associated access module cannot be shorter than the total response timeout timer of all HWTACACS servers in the scheme. Any violation will result in user logoffs before the authentication, authorization, or accounting process is complete.

Examples

In HWTACACS scheme **hwt1**, set the HWTACACS server response timeout timer to 30 seconds.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] timer response-timeout 30
```

Related commands

display hwtacacs scheme

user-name-format (HWTACACS scheme view)

Use **user-name-format** to specify the format of the username to be sent to an HWTACACS server.

Use **undo user-name-format** to restore the default.

Syntax

user-name-format { **keep-original** | **with-domain** | **without-domain** }

undo user-name-format

Default

The ISP domain name is included in the usernames sent to an HWTACACS server.

Views

HWTACACS scheme view

Predefined user roles

network-admin

Parameters

keep-original: Sends the username to the HWTACACS server as the username is entered.

with-domain: Includes the ISP domain name in the username sent to the HWTACACS server.

without-domain: Excludes the ISP domain name from the username sent to the HWTACACS server.

Usage guidelines

A username is generally in the *userid@isp-name* format, of which the *isp-name* argument is used by the device to determine the ISP domain to which a user belongs. However, some HWTACACS servers cannot recognize a username containing an ISP domain name. Before sending a username including a domain name to such an HWTACACS server, the device must remove the domain name. This command allows you to specify whether to include a domain name in a username to be sent to an HWTACACS server.

If an HWTACACS scheme defines that the username is sent without the ISP domain name, do not apply the scheme to more than one ISP domain. Otherwise, the HWTACACS server will consider two users in different ISP domains but with the same *userid* as one user.

Examples

In HWTACACS scheme **hwt1**, configure the device to remove the ISP domain name from the usernames sent to the HWTACACS servers.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] user-name-format without-domain
```

Related commands

display hwtacacs scheme

LDAP commands

attribute-map

Use **attribute-map** to specify the LDAP attribute map in an LDAP scheme.

Use **undo attribute-map** to restore the default.

Syntax

attribute-map *map-name*

undo attribute-map

Default

An LDAP scheme does not use an LDAP attribute map.

Views

LDAP scheme view

Predefined user roles

network-admin

Parameters

map-name: Specifies an LDAP attribute map by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

When the LDAP scheme used for authorization contains an LDAP attribute map, the device converts server-assigned LDAP attributes to device-recognizable AAA attributes based on the mapping entries.

You can specify only one LDAP attribute map in an LDAP scheme. If you execute this command multiple times, the most recent configuration takes effect.

If you specify another attribute map or change the mapping entries, the new settings take effect only on the LDAP authorization that occurs after your operation.

Examples

Specify LDAP attribute map **map1** in LDAP scheme **test**.

```
<Sysname> system-view
[Sysname] ldap scheme test
[Sysname-ldap-test] attribute-map map1
```

Related commands

display ldap-scheme

ldap attribute-map

authentication-server

Use **authentication-server** to specify the LDAP authentication server for an LDAP scheme.

Use **undo authentication-server** to restore the default.

Syntax

authentication-server *server-name*

undo authentication-server

Default

No LDAP authentication server is specified for an LDAP scheme.

Views

LDAP scheme view

Predefined user roles

network-admin

Parameters

server-name: Specifies the name of an LDAP server, a case-insensitive string of 1 to 64 characters.

Usage guidelines

You can specify only one LDAP authentication server in an LDAP scheme. If you execute this command multiple times, the most recent configuration takes effect.

Examples

In LDAP scheme **ldap1**, specify the LDAP authentication server as **ccc**.

```
<Sysname> system-view
[Sysname] ldap scheme ldap1
[Sysname-ldap-ldap1] authentication-server ccc
```

Related commands

display ldap scheme

ldap server

authorization-server

Use **authorization-server** to specify the LDAP authorization server for an LDAP scheme.

Use **undo authorization-server** to restore the default.

Syntax

authorization-server *server-name*

undo authorization-server

Default

No LDAP authorization server is specified for an LDAP scheme.

Views

LDAP scheme view

Predefined user roles

network-admin

Parameters

server-name: Specifies the name of an LDAP server, a case-insensitive string of 1 to 64 characters.

Usage guidelines

You can specify only one LDAP authorization server in an LDAP scheme. If you execute this command multiple times, the most recent configuration takes effect.

Examples

In LDAP scheme **ldap1**, specify the LDAP authorization server as **ccc**.

```
<Sysname> system-view
[Sysname] ldap scheme ldap1
[Sysname-ldap-ldap1] authorization-server ccc
```

Related commands

display ldap scheme

ldap server

display ldap scheme

Use **display ldap scheme** to display LDAP scheme configuration.

Syntax

display ldap scheme [*ldap-scheme-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ldap-scheme-name: Specifies an LDAP scheme by its name, a case-insensitive string of 1 to 32 characters. If you do not specify an LDAP scheme, this command displays the configuration of all LDAP schemes.

Examples

Display the configuration of all LDAP schemes.

```
<Sysname> display ldap scheme
Total 1 LDAP schemes

------------------------------------------------------------------
LDAP scheme name             : aaa
  Authentication server      : aaa
    IP                       : 1.1.1.1
    Port                     : 111
    VPN instance             : Not configured
    LDAP protocol version    : LDAPv3
    Server timeout interval  : 10 seconds
    Login account DN         : Not configured
    Base DN                  : Not configured
    Search scope             : all-level
    User searching parameters:
      User object class      : Not configured
```

```
    Username attribute     : cn
    Username format        : with-domain
 Authorization server      : aaa
   IP                      : 1.1.1.1
   Port                    : 111
   VPN instance            : Not configured
   LDAP protocol version   : LDAPv3
   Server timeout interval : 10 seconds
   Login account DN        : Not configured
   Base DN                 : Not configured
   Search scope            : all-level
   User searching parameters:
     User object class     : Not configured
     Username attribute    : cn
     Username format       : with-domain
 Attribute map             : map1
-------------------------------------------------------------------
```

Table 15 Command output

Field	Description
Authentication server	Name of the LDAP authentication server. If no server is configured, this field displays **Not configured**.
Authorization server	Name of the LDAP authorization server. If no server is configured, this field displays **Not configured**.
IP	IP address of the LDAP server. If no server is specified, this field displays **Not configured**.
Port	Port number of the server. If no port number is specified, this field displays the default port number.
VPN instance	This field is not supported in the current software version. MPLS L3VPN instance to which the LDAP server belongs. If no VPN instance is specified, this field displays **Not configured**.
LDAP protocol version	LDAP version, LDAPv2 or LDAPv3.
Server timeout interval	LDAP server timeout period, in seconds.
Login account DN	DN of the administrator.
Base DN	Base DN for user search.
Search scope	User DN search scope, including: • **all-level**—All subdirectories. • **single-level**—Next lower level of subdirectories under the base DN.
User searching parameters	User search parameters.
User object class	User object class for user DN search. If no user object class is configured, this field displays **Not configured**.
Username attribute	User account attribute for login.
Username format	Format for the username sent to the server.
Attribute map	LDAP attribute map used by the scheme. If no LDAP attribute map is used, this field displays **Not configured**.

ip

Use **ip** to configure the IP address of the LDAP server.

Use **undo ip** to restore the default.

Syntax

ip *ip-address* [**port** *port-number*]

undo ip

Default

An LDAP server does not have an IP address.

Views

LDAP server view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address of the LDAP server.

port *port-number*: Specifies the TCP port number of the LDAP server. The value range for the *port-number* argument is 1 to 65535, and the default value is 389.

Usage guidelines

The LDAP service port configured on the device must be consistent with the service port of the LDAP server.

If you change the IP address and port number of the LDAP server, the change takes effect only on the LDAP authentication that occurs after the change.

Examples

Specify the IP address and port number as 192.168.0.10 and 4300 for LDAP server **ccc**.

```
<Sysname> system-view
[Sysname] ldap server ccc
[Sysname-ldap-server-ccc] ip 192.168.0.10 port 4300
```

Related commands

ldap server

ipv6

Use **ipv6** to configure the IPv6 address of the LDAP server.

Use **undo ipv6** to restore the default.

Syntax

ipv6 *ipv6-address* [**port** *port-number*]

undo ipv6

Default

An LDAP server does not have an IPv6 address.

Views

LDAP server view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the IPv6 address of the LDAP server.

port *port-number*: Specifies the TCP port number of the LDAP server. The value range for the *port-number* argument is 1 to 65535, and the default value is 389.

Usage guidelines

The LDAP service port configured on the device must be consistent with the service port of the LDAP server.

If you change the IP address and port number of the LDAP server, the change takes effect only on the LDAP authentication that occurs after the change.

Examples

Specify the IPv6 address and port number as 1:2::3:4 and 4300 for LDAP server **ccc**.

```
<Sysname> system-view
[Sysname] ldap server ccc
[Sysname-ldap-server-ccc] ipv6 1:2::3:4 port 4300
```

Related commands

ldap server

ldap attribute-map

Use **ldap attribute-map** to create an LDAP attribute map and enter its view, or enter the view of an existing LDAP attribute map.

Use **undo ldap attribute-map** to delete an LDAP attribute map.

Syntax

ldap attribute-map *map-name*

undo ldap attribute-map *map-name*

Default

No LDAP attribute maps exist.

Views

System view

Predefined user roles

network-admin

Parameters

map-name: Specifies the name of the LDAP attribute map, a case-insensitive string of 1 to 31 characters.

Usage guidelines

Execute this command multiple times to create multiple LDAP attribute maps. You can add multiple mapping entries to an LDAP attribute map. Each entry defines the mapping between an LDAP attribute and an AAA attribute.

Examples

Create an LDAP attribute map named **map1** and enter LDAP attribute map view.

```
<Sysname> system-view
[Sysname] ldap attribute-map map1
[Sysname-ldap-map-map1]
```

Related commands

attribute-map

ldap scheme

map

ldap scheme

Use **ldap scheme** to create an LDAP scheme and enter its view, or enter the view of an existing LDAP scheme.

Use **undo ldap scheme** to delete an LDAP scheme.

Syntax

ldap scheme *ldap-scheme-name*

undo ldap scheme *ldap-scheme-name*

Default

No LDAP schemes exist.

Views

System view

Predefined user roles

network-admin

Parameters

ldap-scheme-name: Specifies the LDAP scheme name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

An LDAP scheme can be used by more than one ISP domain at the same time.

You can configure a maximum of 16 LDAP schemes.

Examples

Create an LDAP scheme named **ldap1** and enter LDAP scheme view.

```
<Sysname> system-view
[Sysname] ldap scheme ldap1
[Sysname-ldap-ldap1]
```

Related commands

display ldap scheme

ldap server

Use **ldap server** to create an LDAP server and enter its view, or enter the view of an existing LDAP server.

Use **undo ldap server** to delete an LDAP server.

Syntax

ldap server *server-name*

undo ldap server *server-name*

Default

No LDAP servers exist.

Views

System view

Predefined user roles

network-admin

Parameters

server-name: Specifies the LDAP server name, a case-insensitive string of 1 to 64 characters.

Examples

Create an LDAP server named **ccc** and enter LDAP server view.

```
<Sysname> system-view
[Sysname] ldap server ccc
[Sysname-ldap-server-ccc]
```

Related commands

display ldap scheme

login-dn

Use **login-dn** to specify the administrator DN.

Use **undo login-dn** to restore the default.

Syntax

login-dn *dn-string*

undo login-dn

Default

No administrator DN is specified.

Views

LDAP server view

Predefined user roles

network-admin

Parameters

dn-string: Specifies the administrator DN for binding with the server, a case-insensitive string of 1 to 255 characters.

Usage guidelines

The administrator DN specified on the device must be consistent with the administrator DN configured on the LDAP server.

If you change the administrator DN, the change takes effect only on the LDAP authentication that occurs after the change.

Examples

Specify the administrator DN as **uid=test, ou=people, o=example, c=city** for LDAP server **ccc**.

```
<Sysname> system-view
[Sysname] ldap server ccc
[Sysname-ldap-server-ccc] login-dn uid=test,ou=people,o=example,c=city
```

Related commands

display ldap scheme

login-password

Use **login-password** to configure the administrator password for binding with the LDAP server during LDAP authentication.

Use **undo login-password** to restore the default.

Syntax

login-password { **cipher** | **simple** } *string*

undo login-password

Default

No administrator password is configured.

Views

LDAP server view

Predefined user roles

network-admin

Parameters

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 128 characters. Its encrypted form is a case-sensitive string of 1 to 201 characters.

Usage guidelines

This command takes effect only after the **login-dn** command is used.

Examples

Specify the administrator password as **abcdefg** in plaintext form for LDAP server **ccc**.

```
<Sysname> system-view
[Sysname] ldap server ccc
[Sysname-ldap-server-ccc] login-password simple abcdefg
```

Related commands

display ldap scheme

login-dn

map

Use **map** to configure a mapping entry in an LDAP attribute map.

Use **undo map** to delete the specified mapping entries from the LDAP attribute map.

Syntax

map ldap-attribute *ldap-attribute-name* [**prefix** *prefix-value* **delimiter** *delimiter-value*] **aaa-attribute** { **user-group** | **user-profile** }

undo map [**ldap-attribute** *ldap-attribute-name*]

Default

An LDAP attribute map does not contain mapping entries.

Views

LDAP attribute map view

Predefined user roles

network-admin

Parameters

ldap-attribute *ldap-attribute-name*: Specifies an LDAP attribute by its name. The *ldap-attribute-name* argument is a case-insensitive string of 1 to 63 characters.

prefix *prefix-value* **delimiter** *delimiter-value*: Specifies a partial value string of the LDAP attribute for attribute mapping. The *prefix-value* argument represents the position where the partial string starts. The prefix is a case-insensitive string of 1 to 7 characters, such as **cn=**. The *delimiter-value* argument represents the position where the partial string ends, such as a comma (,). If you do not specify the **prefix** *prefix-value* **delimiter** *delimiter-value* option, the mapping entry uses the entire value string of the LDAP attribute.

aaa-attribute: Specifies an AAA attribute.

user-group: Specifies the user group attribute.

user-profile: Specifies the user profile attribute.

Usage guidelines

Because the device ignores unrecognized LDAP attributes, configure the mapping entries to include important LDAP attributes that should not be ignored.

An LDAP attribute can be mapped only to one AAA attribute. Different LDAP attributes can be mapped to the same AAA attribute.

If you do not specify an LDAP attribute for the **undo map** command, the command deletes all mapping entries from the LDAP attribute map.

Examples

In LDAP attribute map **map1**, map a partial value string of the LDAP attribute named **memberof** to AAA attribute named **user-group**.

```
<Sysname> system-view
[Sysname] ldap attribute-map map1
[Sysname-ldap-map-map1] map ldap-attribute memberof prefix cn= delimiter , aaa-attribute user-group
```

Related commands

ldap attribute-map

user-group

user-profile

protocol-version

Use **protocol-version** to specify the LDAP version.

Use **undo protocol-version** to restore the default.

Syntax

protocol-version { **v2** | **v3** }

undo protocol-version

Default

The LDAP version is LDAPv3.

Views

LDAP server view

Predefined user roles

network-admin

Parameters

v2: Specifies the LDAP version LDAPv2.

v3: Specifies the LDAP version LDAPv3.

Usage guidelines

For successful LDAP authentication, the LDAP version used by the device must be consistent with the version used by the LDAP server.

If you change the LDAP version, the change takes effect only on the LDAP authentication that occurs after the change.

A Microsoft LDAP server supports only LDAPv3.

Examples

Specify the LDAP version as LDAPv2 for LDAP server **ccc**.

```
<Sysname> system-view
[Sysname] ldap server ccc
[Sysname-ldap-server-ccc] protocol-version v2
```

Related commands

display ldap scheme

search-base-dn

Use **search-base-dn to** specify the base DN for user search.

Use **undo search-base-dn** to restore the default.

Syntax

search-base-dn *base-dn*

undo search-base-dn

Default

No base DN is specified for user search.

Views

LDAP server view

Predefined user roles

network-admin

Parameters

base-dn: Specifies the base DN for user search, a case-insensitive string of 1 to 255 characters.

Examples

Specify the base DN for user search as **dc=ldap,dc=com** for LDAP server **ccc**.

```
<Sysname> system-view
[Sysname] ldap server ccc
[Sysname-ldap-server-ccc] search-base-dn dc=ldap,dc=com
```

Related commands

display ldap scheme

ldap server

search-scope

Use **search-scope** to specify the user search scope.

Use **undo search-scope** to restore the default.

Syntax

search-scope { **all-level** | **single-level** }

undo search-scope

Default

The user search scope is **all-level**.

Views

LDAP server view

Predefined user roles

network-admin

Parameters

all-level: Specifies that the search goes through all subdirectories of the base DN.

single-level: Specifies that the search goes through only the next lower level of subdirectories under the base DN.

Examples

Specify the search scope for the LDAP authentication as all subdirectories of the base DN for LDAP server **ccc**.

```
<Sysname> system-view
[Sysname] ldap server ccc
[Sysname-ldap-server-ccc] search-scope all-level
```

Related commands

display ldap scheme

ldap server

server-timeout

Use **server-timeout** to set the LDAP server timeout period, the maximum time that the device waits for an LDAP response.

Use **undo server-timeout** to restore the default.

Syntax

server-timeout *time-interval*

undo server-timeout

Default

The LDAP server timeout period is 10 seconds.

Views

LDAP server view

Predefined user roles

network-admin

Parameters

time-interval: Specifies the LDAP server timeout period in the range of 5 to 20 seconds.

Usage guidelines

If you change the LDAP server timeout period, the change takes effect only on the LDAP authentication that occurs after the change.

Examples

Set the LDAP server timeout period to 15 seconds for LDAP server **ccc**.

```
<Sysname> system-view
[Sysname] ldap server ccc
[Sysname-ldap-server-ccc] server-timeout 15
```

Related commands

display ldap scheme

user-parameters

Use **user-parameters** to configure LDAP user attributes, including the username attribute, username format, and user-defined user object class.

Use **undo user-parameters** to restore the default of an LDAP user attribute.

Syntax

user-parameters { **user-name-attribute** { *name-attribute* | **cn** | **uid** } | **user-name-format** { **with-domain** | **without-domain** } | **user-object-class** *object-class-name* }

undo user-parameters { **user-name-attribute** | **user-name-format** | **user-object-class** }

Default

The LDAP username attribute is **cn** and the username format is **without-domain**. No user object class is specified and the default user object class of the LDAP server is used.

Views

LDAP server view

Predefined user roles

network-admin

Parameters

user-name-attribute { *name-attribute* | **cn** | **uid** }: Specifies the username attribute. The *name-attribute* argument represents an attribute value, a case-insensitive string of 1 to 64 characters. The **cn** keyword represents the user account attribute of common name, and the **uid** keyword represents the user account attribute of user ID.

user-name-format { **with-domain** | **without-domain** }: Specifies the format of the username to be sent to the server. The **with-domain** keyword means that the username contains the domain name, and the **without-domain** keyword means that the username does not contain the domain name.

user-object-class *object-class-name*: Specifies the user object class for user search. The *object-class-name* argument represents a class value, a case-insensitive string of 1 to 64 characters.

Usage guidelines

If the username on the LDAP server does not contain the domain name, specify the **without-domain** keyword. If the username contains the domain name, specify the **with-domain** keyword.

Examples

Set the user object class to **person** for LDAP server **ccc**.

```
<Sysname> system-view
[Sysname] ldap server ccc
[Sysname-ldap-server-ccc] user-parameters user-object-class person
```

Related commands

display ldap scheme

login-dn

RADIUS server commands

display radius-server active-client

Use **display radius-server active-client** to display information about activated RADIUS clients.

Syntax

display radius-server active-client

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display information about all activated RADIUS clients.

```
<Sysname> display radius-server active-client
Total 2 RADIUS clients.
Client IP: 2.2.2.2
Client IP: 3.3.3.3
```

Related commands

radius-server client

display radius-server active-user

Use **display radius-server active-user** to display information about activated RADIUS users.

Syntax

display radius-server active-user [*user-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

user-name: Specifies a RADIUS user name, a case-sensitive string of 1 to 55 characters. The name must meet the following requirements:

- Cannot contain a domain name.
- Cannot contain any of the following characters: forward slash (/), backslash (\), vertical bar (|), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@).
- Cannot be **a**, **al**, or **all**.

If you do not specify a RADIUS user name, this command displays information about all RADIUS users.

Examples

Display information about the activated RADIUS user named **test**.

```
<Sysname> display radius-server active-user test
Total 1 RADIUS users matched.

Username: test
  Description: A network access user from company cc
  Authorization attributes:
    VLAN ID: 2
    ACL number: 2000
  Validity period:
    Expiration time: 2015/04/03-18:00:00
```

Display information about all activated RADIUS users.

```
<Sysname> display radius-server active-user
```

```
Total 2 RADIUS users matched.

Username: 123
  Description: A network access user from company cc
  Authorization attributes:
    VLAN ID: 2
    ACL number: 3000
  Validity period:
    Expiration time: 2016/04/03-18:00:00

Username: 456
  Description: A network access user from company cc
  Authorization attributes:
    VLAN ID: 2
    ACL number: 3000
  Validity period:
    Expiration time: 2016/04/03-18:00:00
```

Table 16 Command output

Field	Description
Username	RADIUS user name.
Description	Description of the RADIUS user.
Authorization attributes	Authorization attributes of the RADIUS user.
VLAN ID	Authorization VLAN.
ACL number	Authorization ACL.
Validity period	Validity time period of the RADIUS user.
Expiration time	Expiration date and time.

Related commands

`local-user`

radius-server activate

Use **`radius-server activate`** to activate the RADIUS server configuration, including RADIUS clients and users.

Syntax

`radius-server activate`

Views

System view

Predefined user roles

network-admin

Usage guidelines

Use this command to immediately activate the most recent RADIUS server configuration after you have added, modified, or deleted RADIUS clients and network access users from which RADIUS user data is generated.

Executing this command restarts the RADIUS server process and an authentication service interruption will occur during the restart.

Examples

Activate the RADIUS server configuration.

```
<Sysname> system-view
[Sysname] radius-server activate
```

Related commands

display radius-server active-client

display radius-server active-user

radius-server client

Use **radius-server client** to configure a RADIUS client.

Use **undo radius-server client** to delete a RADIUS client.

Syntax

radius-server client ip *ipv4-address* **key** { **cipher** | **simple** } *string*

undo radius-server client { **all** | **ip** *ipv4-address* }

Default

No RADIUS clients are specified.

Views

System view

Predefined user roles

network-admin

Parameters

ip *ipv4-address*: Specifies the IPv4 address of the RADIUS client, which must be a Class A, B, or C address and the first octet cannot be 0 or 127.

key: Specifies the shared key to communicate with the RADIUS client.

cipher: Specifies the key in encrypted form.

simple: Specifies the key in plaintext form.

string: Specifies a case-sensitive key string. The encrypted form of the key is a string of 1 to 117 characters. The plaintext form of the key is a string of 1 to 64 characters.

all: Specifies all RADIUS clients.

Usage guidelines

The IP address of a RADIUS client must be the same as the source IP address for outgoing RADIUS packets specified on the RADIUS client.

The shared key of a RADIUS client must be the same as the setting on the RADIUS client.

Execute this command multiple times to configure multiple RADIUS clients.

Examples

Configure a RADIUS client whose IP address is 2.2.2.2 and shared key is **test** in plaintext.

```
<Sysname> system-view
[Sysname] radius-server client ip 2.2.2.2 key simple test
```

Related commands

display radius-server active-client

Connection recording policy commands

aaa connection-recording policy

Use **aaa connection-recording policy** to create a connection recording policy and enter its view, or enter the view of an existing connection recording policy.

Use **aaa connection-recording policy** to delete the connection recording policy.

Syntax

aaa connection-recording policy

undo aaa connection-recording policy

Default

The connection recording policy does not exist.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Use this feature on scenarios where the device acts as an FTP, SSH, SFTP, or Telnet login client to establish a connection with a login server. This feature enables the device to provide an accounting server with the connection start and termination information. When the login client establishes a connection with the login server, the system sends a start-accounting request to the accounting server. When the connection is terminated, the system sends a stop-accounting request to the accounting server.

Examples

Create a connection recording policy and enter its view.

```
<Sysname> system-view
[Sysname] aaa connection-recording policy
[sysname-connection-recording-policy]
```

Related commands

accounting hwtacacs-scheme

display aaa connection-recording policy

accounting hwtacacs-scheme

Use **accounting hwtacacs-scheme** to specify the accounting method for the connection recording policy.

Use **undo accounting** to restore the default.

Syntax

accounting hwtacacs-scheme *hwtacacs-scheme-name*

undo accounting

Default

No accounting method is specified for the connection recording policy. No accounting is performed on the connections initiated by the device as a login client.

Views

Connection recording policy view

Predefined user roles

network-admin

Parameters

hwtacacs-scheme-name: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

If the accounting method is changed, the new method takes effect only on subsequent connections initiated by the device as a login client.

For a connection, once the device sends the start-accounting request to an HWTACACS server, it sends the connection's stop-accounting packet to the same server.

If you execute this command multiple times, the most recent configuration takes effect.

The device includes the username entered by a user in the accounting packets to be sent to the AAA server for connection recording. The username format configured by using the **user-name-format** command in the accounting scheme does not take effect.

Examples

Create a connection recording policy, and specify HWTACACS scheme **tac** as the accounting method.

```
<Sysname> system-view
[Sysname] aaa connection-recording policy
[sysname-connection-recording-policy] accounting hwtacacs-scheme tac
```

Related commands

aaa connection-recording policy

display aaa connection-recording policy

display aaa connection-recording policy

Use **display aaa connection-recording policy** to display the connection recording policy configuration.

Syntax

display aaa connection-recording policy

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the connection recording policy configuration.

```
<Sysname> display aaa connection-recording policy
Connection-recording policy:
  Accounting scheme: HWTACACS=tac1
```

Related commands

aaa connection-recording policy

accounting hwtacacs-scheme

Contents

802.1X commands

display dot1x

Use **display dot1x** to display information about 802.1X.

Syntax

display dot1x [**sessions** | **statistics**] [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

sessions: Displays 802.1X session information.

statistics: Displays 802.1X statistics.

interface *interface-type interface-number*: Specifies a port by its type and number.

Usage guidelines

If you do not specify the **sessions** keyword or the **statistics** keyword, this command displays all information about 802.1X, including session information, statistics, and settings.

If you do not specify the **interface** *interface-type interface-number* option, this command displays all global and port-specific 802.1X information.

Examples

Display all information about 802.1X.

```
<Sysname> display dot1x
Global 802.1X parameters:
   802.1X authentication               : Enabled
   EAP authentication                  : Enabled
   Max-tx period                       : 30 s
   Handshake period                    : 15 s
   Quiet timer                         : Disabled
         Quiet period                  : 60 s
   Supp timeout                        : 30 s
   Server timeout                      : 100 s
   Reauth period                       : 3600 s
   Max auth requests                   : 2
   User aging period for Auth-Fail VLAN : 1000 s
   User aging period for critical VLAN  : 1000 s
   User aging period for guest VLAN     : 1000 s
   EAD assistant function              : Disabled
       Permit authentication-escape    : Disabled
       URL                             : http://www.dwsoft.com
```

```
      Free IP                          : 6.6.6.0         255.255.255.0
      EAD timeout                      : 30 min
  Domain delimiter                     : @
  Max EAP-TLS fragment (to-server)     : 400 bytes
Online 802.1X wired users              : 1

GigabitEthernet1/0/1  is link-up
  802.1X authentication            : Enabled
  Handshake                        : Enabled
  Handshake reply                  : Disabled
  Handshake security               : Disabled
  Unicast trigger                  : Disabled
  Periodic reauth                  : Disabled
  Port role                        : Authenticator
  Authorization mode               : Auto
  Port access control              : MAC-based
  Multicast trigger                : Enabled
  Mandatory auth domain            : Not configured
  Guest VLAN                       : 3
  Auth-Fail VLAN                   : Not configured
  Critical VLAN                    : Not configured
  Critical voice VLAN              : Disabled
  Add Guest VLAN delay             : Disabled
  Re-auth server-unreachable       : Logoff
  Max online users                 : 4294967295
  User IP freezing                 : Disabled
  Reauth period                    : 0 s
  Send Packets Without Tag         : Disabled
  Max Attempts Fail Number         : 0
  User aging                       : Enabled
  Server-recovery online-user-sync : Enabled
  Auth-Fail EAPOL                  : Disabled
  Critical EAPOL                   : Disabled
  Discard duplicate EAPOL-Start    : No

  EAPOL packets: Tx 3, Rx 3
  Sent EAP Request/Identity packets : 1
       EAP Request/Challenge packets: 1
       EAP Success packets: 1
       EAP Failure packets: 0
  Received EAPOL Start packets : 1
           EAPOL LogOff packets: 1
           EAP Response/Identity packets : 1
           EAP Response/Challenge packets: 1
           Error packets: 0
  Online 802.1X users: 1
         MAC address         Auth state
         0001-0000-0000      Authenticated
```

Table 1 Command output

Field	Description
Global 802.1X parameters	Global 802.1X configuration.
802.1X authentication	Whether 802.1X is enabled globally.
CHAP authentication	Performs EAP termination and uses CHAP to communicate with the RADIUS server.
EAP authentication	Relays EAP packets and supports any of the EAP authentication methods to communicate with the RADIUS server.
PAP authentication	Performs EAP termination and uses PAP to communicate with the RADIUS server.
Max-tx period	Username request timeout timer in seconds.
Handshake period	Handshake timer in seconds.
Quiet timer	Status of the quiet timer, enabled or disabled.
Quiet period	Quiet timer in seconds.
Supp timeout	Client timeout timer in seconds.
Server timeout	Server timeout timer in seconds.
Reauth period	Periodic reauthentication timer in seconds.
Max auth requests	Maximum number of attempts for sending an authentication request to a client.
User aging period for Auth-Fail VLAN	Aging timer in seconds for users in Auth-Fail VLANs.
User aging period for critical VLAN	Aging timer in seconds for users in critical VLANs.
User aging period for guest VLAN	Aging timer in seconds for users in guest VLANs.
EAD assistant function	Whether EAD assistant is enabled.
Permit authentication-escape	This field is supported only in Release 6331 and later. Whether 802.1X Auth-Fail and critical VLANs and MAC authentication critical VLANs are supported when 802.1X EAD assistant is enabled.
URL	Redirect URL for unauthenticated users using a Web browser to access the network.
Free IP	Network segment accessible to unauthenticated users.
EAD timeout	EAD rule timer in minutes.
Domain delimiter	Domain delimiters supported by the device.
Max EAP-TLS fragment (to-server)	Maximum size of EAP-TLS fragments sent in authentication packets to the server. If no maximum size is set, this field displays N/A.
Online 802.1X wired users	Number of wired online 802.1X users, including users that have passed 802.1X authentication and users that are performing 802.1X authentication.
GigabitEthernet1/0/1 is link-up	Status of the port. In this example, GigabitEthernet 1/0/1 is up.
802.1X authentication	Whether 802.1X is enabled on the port.
Handshake	Whether the online user handshake feature is enabled on the port.
Handshake reply	Whether the online user handshake reply feature is enabled on the

Field	Description
	port.
Handshake security	Whether the online user handshake security feature is enabled on the port.
Unicast trigger	Whether the 802.1X unicast trigger is enabled on the port.
Periodic reauth	Whether 802.1X periodic reauthentication is enabled on the port.
Port role	Role of the port. The port functions only as an **Authenticator**.
Authorization mode	Authorization state of the port, which can be Force-Authorized, Auto, or Force-Unauthorized.
Port access control	Access control method of the port: • **MAC-based**—MAC-based access control. • **Port-based**—Port-based access control.
Multicast trigger	Whether the 802.1X multicast trigger feature is enabled.
Mandatory auth domain	Mandatory authentication domain on the port.
Guest VLAN	802.1X guest VLAN configured on the port. If no 802.1X guest VLAN is configured on the port, this field displays **Not configured**.
Auth-Fail VLAN	802.1X Auth-Fail VLAN configured on the port. If no 802.1X Auth-Fail VLAN is configured on the port, this field displays **Not configured**.
Critical VLAN	802.1X critical VLAN configured on the port. If no 802.1X critical VLAN is configured on the port, this field displays **Not configured**.
Critical voice VLAN	Whether the 802.1X critical voice VLAN feature is enabled on the port.
Add Guest VLAN delay	Status and mode of the 802.1X guest VLAN assignment delay feature on a port: • **EAPOL**—EAPOL-triggered 802.1X guest VLAN assignment delay is enabled. • **NewMac**—New MAC-triggered 802.1X guest VLAN assignment delay is enabled. • **ALL**—Both EAPOL-triggered and new MAC-triggered 802.1X guest VLAN assignment delays are enabled. • **Disabled**—802.1X guest VLAN assignment delay is disabled.
Re-auth server-unreachable	Whether to log off online 802.1X users or keep them online when no server is reachable for 802.1X reauthentication.
Max online users	Maximum number of concurrent 802.1X users on the port.
User IP freezing	Whether user IP freezing is enabled on the port.
Reauth period	Periodic reauthentication timer in seconds on the port.
Send Packets Without Tag	Whether to remove the VLAN tags of all 802.1X protocol packets sent out of the port to 802.1X clients.
Max Attempts Fail Number	Maximum number of 802.1X authentication attempts for MAC authenticated users.
User aging	Status of 802.1X unauthenticated user aging on a port: • Enabled. • Disabled.

Field	Description
Server-recovery online-user-sync	Status of 802.1X online user synchronization: • Enabled. • Disabled.
Auth-Fail EAPOL	This field is not supported in the current software version. This field displays whether the device sends EAP-Success packets to 802.1X clients on their assignment to the 802.1X Auth-Fail VLAN on the port.
Critical EAPOL	This field displays whether the device sends EAP-Success packets to 802.1X clients on their assignment to the 802.1X critical VLAN on the port.
Discard duplicate EAPOL-Start	Whether the device discards duplicate 802.1X EAPOL-Start packets: • **Yes**—The device discards duplicate 802.1X EAPOL-Start packets. • **No**—The device does not discard duplicate 802.1X EAPOL-Start packets.
EAPOL packets	Number of sent (Tx) and received (Rx) EAPOL packets.
Sent EAP Request/Identity packets	Number of sent EAP-Request/Identity packets.
EAP Request/Challenge packets	Number of sent EAP-Request/MD5-Challenge packets.
EAP Success packets	Number of sent EAP-Success packets.
EAP Failure packets	Number of sent EAP-Failure packets.
Received EAPOL Start packets	Number of received EAPOL-Start packets.
EAPOL LogOff packets	Number of received EAPOL-LogOff packets.
EAP Response/Identity packets	Number of received EAP-Response/Identity packets.
EAP Response/Challenge packets	Number of received EAP-Response/MD5-Challenge packets.
Error packets	Number of received error packets.
Online 802.1X users	Number of online 802.1X users on the port, including users that have passed 802.1X authentication and users that are performing 802.1X authentication.
MAC address	MAC addresses of the online 802.1X users.
Auth state	Authentication status of the online 802.1X users.

display dot1x connection

Use **display dot1x connection** to display information about online 802.1X users.

Syntax

display dot1x connection [**open**] [**interface** *interface-type interface-number* | **slot** *slot-number* | **user-mac** *mac-address* | **user-name** *name-string*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

open: Displays information only about 802.1X users that use nonexistent usernames or incorrect passwords for network access in open authentication mode. If you do not specify this keyword, the command displays information about all online 802.1X users.

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify a port, this command displays online 802.1X user information for all ports.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays online 802.1X user information for all member devices.

user-mac *mac-address*: Specifies an 802.1X user by MAC address. The *mac-address* argument represents the MAC address of the user, in the form of H-H-H. If you do not specify an 802.1X user, this command displays all online 802.1X user information.

user-name *name-string*: Specifies an 802.1X user by its name. The *name-string* argument represents the username, a case-sensitive string of 1 to 253 characters. If you do not specify an 802.1X user, this command displays all online 802.1X user information.

Examples

Display information about all online 802.1X users.

```
<Sysname> display dot1x connection
Total connections: 1

Slot ID: 1
User MAC address: 0015-e9a6-7cfe
Access interface: GigabitEthernet1/0/1
Username: ias
User access state: Successful
Authentication domain: h3c
IPv4 address: 192.168.1.1
IPv6 address: 2000:0:0:0:1:2345:6789:abcd
Authentication method: CHAP
AAA authentication method: Local
Initial VLAN: 1
Authorization untagged VLAN: 6
Authorization tagged VLAN list: 1 to 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 29 31 33
                                35 37 40 to 100
Authorization VSI: N/A
Authorization ACL number/name: 3001
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Default
Session timeout period: 2 s
Packet detection:
  Max attempts: 5
  Remaining attempts: 3
  Source IPv4 address: 192.168.1.3
  Source IPv4 mask: 255.255.0.0
```

```
Online from: 2013/03/02  13:14:15
Online duration: 0h 2m 15s
```

Table 2 Command output

Field	Description
Total connections	Number of online 802.1X users.
User MAC address	MAC address of the user.
Access interface	Interface through which the user access the device.
User access state	Access state of the user. • **Successful**—The user passes 802.1X authentication and comes online. • **Open**—The user uses a nonexistent username or an incorrect password to come online in open authentication mode.
Authentication domain	ISP domain used for 802.1X authentication.
IPv4 address	IPv4 address of the user. If the device does not get the IPv4 address of the user, this field is not available.
IPv6 address	IPv6 address of the user. If the device does not get the IPv6 address of the user, this field is not available.
Authentication method	EAP message handling method: • **CHAP**—Performs EAP termination and uses CHAP to communicate with the RADIUS server. • **EAP**—Relays EAP packets and supports any of the EAP authentication methods to communicate with the RADIUS server. • **PAP**—Performs EAP termination and uses PAP to communicate with the RADIUS server.
AAA authentication method	This field is supported only in Release 6340 or later. AAA authentication method for the user to come online: • **Local**—Local authentication. • **HWTACACS**—HWTACACS authentication. • **RADIUS**—RADIUS authentication. • **None**—No authentication was performed.
Initial VLAN	VLAN to which the user belongs before 802.1X authentication.
Authorization untagged VLAN	Untagged VLAN assigned to the user. The VLAN assigned by the server to a user as an authorization VLAN might have been configured on the user access port but with a different tagging mode. For example, the server assigns an authorization VLAN with a tagged attribute, but the same VLAN configured on the port has an untagged attribute. In this situation, if the link type of the port is hybrid, the VLAN settings configured on the port take effect on the user. For more information, see 802.1X in *Security Configuration Guide*.
Authorization tagged VLAN list	Tagged VLANs assigned to the user. The VLAN assigned by the server to a user as an authorization VLAN might have been configured on the user access port but with a different tagging mode. For example, the server assigns an authorization VLAN with a tagged attribute, but the same VLAN configured on the port has an untagged attribute. In this situation, if the link type of the port is hybrid, the VLAN settings configured on the port take effect on the user.

Field	Description
	For more information, see 802.1X in *Security Configuration Guide*.
Authorization VSI	This field is not supported in the current software version. VSI assigned to the user.
Authorization ACL number/name	Number or name of the static ACL assigned to the user. If no static ACL has been assigned, this field displays **N/A**. If the ACL assignment fails, this field displays **(NOT effective)** next to the ACL number or name.
Authorization dynamic ACL name	This field is supported only in Release 6331 and later. Name of the dynamic ACL assigned to the user. If no dynamic ACL is assigned to the user, this field displays **N/A**. If the ACL assignment fails, this field displays **(NOT effective)** next to the ACL name.
Authorization user profile	User profile assigned to the user.
Authorization CAR	This field is not supported in the current software version. Authorization CAR attributes assigned by the server. If no authorization CAR attributes are assigned, this field displays **N/A**.
Authorization URL	Redirect URL assigned to the user.
Termination action	Action attribute assigned by the server to terminate the user session: • **Default**—Logs off the online authenticated 802.1X user when the server-assigned session timeout timer expires. This attribute does not take effect when 802.1X periodic reauthentication is enabled and the periodic reauthentication timer is shorter than the server-assigned session timeout timer. • **Radius-request**—Reauthenticates the online user when the server-assigned session timeout timer expires, regardless of whether the 802.1X periodic reauthentication feature is enabled or not. If the device performs local authentication, this field displays **Default**.
Session timeout period	Session timeout timer assigned by the server.
Packet detection	This field is supported only in Release 6348P01 or later. Information about the packet detection feature.
Max attempts	This field is supported only in Release 6348P01 or later. Maximum number of attempts for sending a detection packet to the user.
Remaining attempts	This field is supported only in Release 6348P01 or later. Remaining number of attempts for sending a detection packet to the user. The device decreases the number by 1 each time it makes an attempt to send the detection packet to the user.
Source IPv4 address	This field is supported only in Release 6348P01 or later. IP address specified for calculating the source IP address of ARP detection packets. If no IP address is specified, this field displays 0.0.0.0.
Source IPv4 mask	This field is supported only in Release 6348P01 or later. Mask specified for calculating the source IP address of ARP detection packets. If no mask is specified, this field displays 0.0.0.0.
Online from	Time from which the 802.1X user came online.

Field	Description
Online duration	Online duration of the 802.1X user.

display dot1x mac-address

Use **display dot1x mac-address** to display the MAC addresses of 802.1X users in a type of 802.1X VLAN.

Syntax

display dot1x mac-address { **auth-fail-vlan** | **critical-vlan** | **guest-vlan** } [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

auth-fail-vlan: Specifies 802.1X Auth-Fail VLANs.

critical-vlan: Specifies 802.1X critical VLANs.

guest-vlan: Specifies 802.1X guest VLANs.

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify a port, this command displays the MAC addresses of 802.1X users in the specified type of 802.1X VLAN on all ports.

Usage guidelines

The displayed MAC addresses and MAC address count might not include all MAC addresses if a large number of 802.1X users are performing authentication frequently.

Examples

Display the MAC addresses of 802.1X users in the 802.1X Auth-Fail VLANs on all ports.

```
<Sysname> display dot1x mac-address auth-fail-vlan
Total MAC addresses: 10
Interface: GigabitEthernet1/0/1        Auth-Fail VLAN: 3    Aging time: N/A
MAC addresses: 8
  0800-2700-9427    0800-2700-2341    0800-2700-2324    0800-2700-2351
  0800-2700-5627    0800-2700-2251    0800-2700-8624    0800-2700-3f51

Interface: GigabitEthernet1/0/2        Auth-Fail VLAN: 5    Aging time: 30 sec
MAC addresses: 2
  0801-2700-9427    0801-2700-2341
```

Table 3 Command output

Field	Description
Total MAC addresses	Total number of MAC addresses in the specified type of VLAN on the specified port or all ports.
Interface	Access port of 802.1X users.

Field	Description
Type VLAN	VLAN that contains the 802.1X users. The *Type* argument has the following values: • Auth-Fail VLAN. • Critical VLAN. • Guest VLAN.
Aging time	MAC address aging time in seconds. This field displays **N/A** if the MAC addresses do not age out.
MAC addresses	Number of matching MAC addresses on a port.
xxxx-xxxx-xxxx	MAC address.

Related commands

dot1x auth-fail vlan

dot1x critical vlan

dot1x guest-vlan

dot1x

Use **dot1x** to enable 802.1X globally or on a port.

Use **undo dot1x** to disable 802.1X globally or on a port.

Syntax

dot1x

undo dot1x

Default

802.1X is neither enabled globally nor enabled for any port.

Views

System view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

For the 802.1X feature to take effect on a port, you must enable the feature both globally and on the port.

Examples

Enable 802.1X globally.

```
<Sysname> system-view
[Sysname] dot1x
```

Enable 802.1X on GigabitEthernet 1/0/1.

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x
[Sysname-GigabitEthernet1/0/1] quit
```

Related commands

display dot1x

dot1x { ip-verify-source | ipv6-verify-source } enable

Use **dot1x** { **ip-verify-source** | **ipv6-verify-source** } **enable** to enable generation of dynamic IPv4SG or IPv6SG binding entries for 802.1X authenticated users.

Use **undo dot1x** { **ip-verify-source** | **ipv6-verify-source** } **enable** to disable generation of dynamic IPv4SG or IPv6SG binding entries for 802.1X authenticated users.

Syntax

dot1x { **ip-verify-source** | **ipv6-verify-source** } **enable**

undo dot1x { **ip-verify-source** | **ipv6-verify-source** } **enable**

Default

Generation of dynamic IPv4SG or IPv6SG binding entries for 802.1X authenticated users is enabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

IMPORTANT:

This feature must operate in conjunction with the IP source guard (IPSG) feature.

This command is supported only in Release 6340 or later.

This command takes effect only on 802.1X users that come online after you execute this command. For existing online 802.1X users, the device updates the dynamic IPv4SG or IPv6SG binding entries for them only when their IP addresses change.

When you execute the **undo** form of this command, the device does not delete the existing dynamic IPv4SG or IPv6SG binding entries for online 802.1X users. Instead, the device deletes the dynamic IPv4SG or IPv6SG binding entry for an online 802.1X user only when the IP address of that user changes.

Examples

Disable generation of dynamic IPv4SG or IPv6SG binding entries for 802.1X authenticated users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo dot1x ip-verify-source enable
```

dot1x access-user log enable

Use **dot1x access-user log enable** to enable 802.1X user logging.

Use **undo dot1x access-user log enable** to disable 802.1X user logging.

Syntax

dot1x access-user log enable [**abnormal-logoff** | **failed-login** | **normal-logoff** | **successful-login**] *

undo dot1x access-user log enable [**abnormal-logoff** | **failed-login** | **normal-logoff** | **successful-login**] *

Default

802.1X user logging is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

abnormal-logoff: Logs exceptional logoffs of 802.1X users, such as logoffs caused by real-time accounting failures or reauthentication failures.

failed-login: Logs 802.1X user login failures.

normal-logoff: Logs logoffs requested by 802.1X users.

successful-login: Logs successful 802.1X user logins.

Usage guidelines

To prevent excessive 802.1X user log entries, use this feature only if you need to analyze abnormal 802.1X user logins or logouts.

If you do not specify any parameters, this command enables all types of 802.1X user logs.

Examples

Enable logging 802.1X user login failures.

```
<Sysname> system-view
[Sysname] dot1x access-user log enable failed-login
```

Related commands

info-center source dot1x logfile deny (*Network Management and Monitoring Command Reference*)

dot1x after-mac-auth max-attempt

Use **dot1x after-mac-auth max-attempt** to set the maximum number of 802.1X authentication attempts for MAC authenticated users on a port.

Use **undo dot1x after-mac-auth max-attempt** to restore the default.

Syntax

dot1x after-mac-auth max-attempt *max-attempts*

undo dot1x after-mac-auth max-attempt

Default

The number of 802.1X authentication attempts for MAC authenticated users is not limited on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

max-attempts: Specifies a number in the range of 1 to 50.

Usage guidelines

The device denies 802.1X authentication requests of a MAC authenticated user after the maximum number of 802.1X authentication attempts has been made.

The device will recount the number of 802.1X authentication attempts made by a MAC authenticated user if a user logoff or device reboot event occurs.

Examples

Configure GigabitEthernet 1/0/1 to allow a maximum of 10 802.1X authentication attempts made by a MAC authenticated user.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x after-mac-auth max-attempt 10
```

Related commands

display dot1x

dot1x authentication-method

Use **dot1x authentication-method** to specify an EAP message handling method.

Use **undo dot1x authentication-method** to restore the default.

Syntax

dot1x authentication-method { **chap** | **eap** | **pap** }

undo dot1x authentication-method

Default

The access device performs EAP termination and uses CHAP to communicate with the RADIUS server.

Views

System view

Predefined user roles

network-admin

Parameters

chap: Configures the access device to perform Extensible Authentication Protocol (EAP) termination and use the Challenge Handshake Authentication Protocol (CHAP) to communicate with the RADIUS server.

eap: Configures the access device to relay EAP packets, and supports any of the EAP authentication methods to communicate with the RADIUS server.

pap: Configures the access device to perform EAP termination and use the Password Authentication Protocol (PAP) to communicate with the RADIUS server.

Usage guidelines

The access device terminates or relays EAP packets.

- **In EAP termination mode**—The access device re-encapsulates and sends the authentication data from the client in standard RADIUS packets to the RADIUS server. The device performs either CHAP or PAP authentication with the RADIUS server. In this mode, the RADIUS server

supports only MD5-Challenge EAP authentication and the username and password EAP authentication initiated by an iNode client.

- PAP transports usernames and passwords in plain text. The authentication method applies to scenarios that do not require high security. To use PAP, the client can be an iNode 802.1X client.
- CHAP transports usernames in plain text and passwords in encrypted form over the network. CHAP is more secure than PAP.

- **In EAP relay mode**—The access device relays EAP messages between the client and the RADIUS server. The EAP relay mode supports multiple EAP authentication methods, such as MD5-Challenge, EAP-TLS, and PEAP. To use this mode, make sure the RADIUS server meets the following requirements:
  - Supports the EAP-Message and Message-Authenticator attributes.
  - Uses the same EAP authentication method as the client.

  If this mode is used, the **user-name-format** command configured in RADIUS scheme view does not take effect. For more information about the **user-name-format** command, see "RADIUS commands."

If RADIUS authentication is used, you must configure the access device to use the same authentication method (PAP, CHAP, or EAP) as the RADIUS server.

Examples

Enable the access device to terminate EAP packets and perform PAP authentication with the RADIUS server.

```
<Sysname> system-view
[Sysname] dot1x authentication-method pap
```

Related commands

display dot1x

dot1x auth-fail vlan

Use **dot1x auth-fail vlan** to configure an 802.1X Auth-Fail VLAN on a port.

Use **undo dot1x auth-fail vlan** to restore the default.

Syntax

dot1x auth-fail vlan *authfail-vlan-id*

undo dot1x auth-fail vlan

Default

No 802.1X Auth-Fail VLAN exists on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

authfail-vlan-id: Specifies the ID of the 802.1X Auth-Fail VLAN on the port. The value range for the VLAN ID is 1 to 4094. Make sure the VLAN has been created.

Usage guidelines

An 802.1X Auth-Fail VLAN accommodates users that have failed 802.1X authentication for any reason other than unreachable servers. Users in the Auth-Fail VLAN can access a limited set of network resources.

To delete a VLAN that has been configured as an 802.1X Auth-Fail VLAN, you must first use the **undo dot1x auth-fail vlan** command.

Examples

Configure VLAN 100 as the Auth-Fail VLAN on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x auth-fail vlan 100
```

Related commands

display dot1x

dot1x critical eapol

Use **dot1x critical eapol** to enable the sending of an EAP-Success packet to a client when the 802.1X client user is assigned to the 802.1X critical VLAN on a port.

Use **undo dot1x critical eapol** to restore the default.

Syntax

dot1x critical eapol

undo dot1x critical eapol

Default

The device sends an EAP-Failure packet to a client when the 802.1X client user is assigned to the 802.1X critical VLAN on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

By default, the device sends EAP-Failure packets to 802.1X clients when the client users are assigned to the 802.1X critical VLAN. Some 802.1X clients, such as Windows built-in 802.1X clients, cannot respond to the EAP-Request/Identity packets from the device for reauthentication if they have received an EAP-Failure packet. As a result, reauthentication for these clients will fail after the authentication server becomes reachable.

To avoid this situation, enable the device to send EAP-Success packets instead of EAP-Failure packets to 802.1X clients when the client users are assigned to the 802.1X critical VLAN.

Examples

Send an EAP-Success packet to a client when the 802.1X client user is assigned to the 802.1X critical VLAN on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x critical eapol
```

Related commands

dot1x critical vlan

dot1x critical vlan

Use **dot1x critical vlan** to configure an 802.1X critical VLAN on a port.

Use **undo dot1x critical vlan** to restore the default.

Syntax

dot1x critical vlan *critical-vlan-id*

undo dot1x critical vlan

Default

No 802.1X critical VLAN exists on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

critical-vlan-id: Specifies the ID of the 802.1X critical VLAN on the port. The value range for the VLAN ID is 1 to 4094. Make sure the VLAN has been created.

Usage guidelines

An 802.1X critical VLAN accommodates users that fail 802.1X authentication because all the RADIUS servers in their ISP domains are unreachable. Users in the critical VLAN can access a limited set of network resources depending on the configuration.

To delete a VLAN that has been configured as an 802.1X critical VLAN, you must first use the **undo dot1x critical vlan** command.

Examples

Specify VLAN 100 as the 802.1X critical VLAN on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x critical vlan 100
```

Related commands

display dot1x

dot1x critical-voice-vlan

Use **dot1x critical-voice-vlan** to enable the 802.1X critical voice VLAN feature on a port.

Use **undo dot1x critical-voice-vlan** to restore the default.

NOTE:

This command is not supported on the following switch series:

- S5000E-X.
- S5110V2-SI.

- S5000V3-EI.
- S5000V5-EI.
- S5000X-EI.
- WAS6000.

Syntax

dot1x critical-voice-vlan

undo dot1x critical-voice-vlan

Default

The 802.1X critical voice VLAN feature is disabled on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

The 802.1X critical voice VLAN on a port accommodates 802.1X voice users that have failed authentication because none of the RADIUS servers in their ISP domain are reachable.

Before you enable the 802.1X critical voice VLAN feature on the port, make sure the following requirements are met:

- The port is configured with the voice VLAN.

  To configure a voice VLAN on a port, use the **voice-vlan enable** command (see *Layer 2—LAN Switching Command Reference*).
- LLDP is enabled both globally and on the port.

  The device uses LLDP to identify voice users. For information about LLDP commands, see *Layer 2—LAN Switching Command Reference*.
- An 802.1X critical VLAN is configured on the port. This setting ensures that a voice user is assigned to the critical VLAN if it has failed authentication for unreachability of RADIUS servers before the device recognizes it as a voice user. If an 802.1X critical VLAN is not available, the voice user might be logged off instead.

Examples

Enable the 802.1X critical voice VLAN feature on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x critical-voice-vlan
```

Related commands

display dot1x

lldp enable (*Layer 2—LAN Switching Command Reference*)

lldp global enable (*Layer 2—LAN Switching Command Reference*)

voice-vlan enable (*Layer 2—LAN Switching Command Reference*)

dot1x duplicate-eapol-start discard

Use **dot1x duplicate-eapol-start discard** to discard duplicate EAPOL-Start requests on an interface.

Use **undo dot1x duplicate-eapol-start discard** to restore the default.

Syntax

dot1x duplicate-eapol-start discard

undo dot1x duplicate-eapol-start discard

Default

The device does not discard duplicate EAPOL-Start requests on an interface if the requests are legal.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

This command is supported only in Release 6309P01 or later.

During 802.1X authentication, the device might receive duplicate EAPOL-Start requests from an 802.1X user. By default, the device delivers the duplicate EAPOL-Start requests to the authentication server as long as they are legal. However, this mechanism might result in authentication failure if the authentication server cannot respond to duplicate EAPOL-Start requests. To resolve this issue, use this command on the user access interface to discard duplicate EAPOL-Start requests.

As a best practice, use this command only if the server cannot respond to duplicate EAPOL-Start requests. Do not use this command in other situations.

Examples

Discard duplicate EAPOL-Start requests on Ten-GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] dot1x duplicate-eapol-start discard
```

Related commands

display dot1x

dot1x domain-delimiter

Use **dot1x domain-delimiter** to specify a set of domain name delimiters supported by the device.

Use **undo dot1x domain-delimiter** to restore the default.

Syntax

dot1x domain-delimiter *string*

undo dot1x domain-delimiter

Default

The device supports only the at sign (@) delimiter for 802.1X users.

Views

System view

Predefined user roles

network-admin

Parameters

string: Specifies a set of 1 to 16 domain name delimiters for 802.1X users. No space is required between delimiters. Available delimiters include the at sign (@), backslash (\), dot (.), and forward slash (/). If you want to use backslash (\) as the domain name delimiter, you must enter the escape character (\) along with the backslash (\) sign.

Usage guidelines

Any character in the configured set can be used as the domain name delimiter for 802.1X authentication users. Usernames that include domain names can use the format of *username*@*domain-name*, *domain-name**username*, *username*.*domain-name*, or *username*/*domain-name*.

The delimiter set you configured overrides the default setting. If the at sign (@) is not included in the delimiter set, the device does not support the 802.1X users that use this sign as the domain name delimiter.

If a username string contains multiple configured delimiters, the device takes the rightmost delimiter in the username string as the domain name delimiter. For example, if you configure the forward slash (/), dot (.), and backslash (\) as delimiters, the domain name delimiter for the username string 121.123/22\@abc is the backslash (\). The username is **@abc** and the domain name is **121.123/22**.

Examples

Specify the at sign (@) and forward slash (/) as domain name delimiters.

```
<Sysname> system-view
[Sysname] dot1x domain-delimiter @/
```

Related commands

display dot1x

dot1x ead-assistant enable

Use **dot1x ead-assistant enable** to enable the EAD assistant feature.

Use **undo dot1x ead-assistant enable** to disable the EAD assistant feature.

NOTE:

The EAD assistant feature is not supported on the following switch series:

- S5000E-X.
- S5110V2-SI.
- S5000V3-EI.
- S5000V5-EI.
- S5000X-EI.
- WAS6000.

Syntax

dot1x ead-assistant enable

undo dot1x ead-assistant enable

Default

The EAD assistant feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The EAD assistant feature enables the access device to redirect the HTTP or HTTPS requests of a user to a URL to download and install EAD client. This feature eliminates the tedious job of the administrator to deploy EAD clients.

For the EAD assistant feature to take effect on a port, you must set the port authorization mode to **auto**.

The feature is mutually exclusive with MAC authentication and port security. You must disable MAC authentication and port security globally before you enable the EAD assistant feature.

As from Release 6331, the **dot1x ead-assistant permit authentication-escape** command is added to remove the 802.1X Auth-Fail VLAN and critical VLAN malfunction issue when EAD assistant is enabled. This command enables the device to remove the EAD entries of users before it assigns the users to 802.1X Auth-Fail and critical VLANs.

As from Release 6328, you can use EAD assistant in conjunction with MAC authentication. When you use both EAD assistant and MAC authentication on the device, follow these restrictions and guidelines:

- If both EAD assistant and MAC authentication are configured, the device does not mark the MAC address of a user that has failed MAC authentication as a silent MAC address. If the user has never passed MAC authentication, packets from the user can trigger MAC authentication again only after the user's EAD entry ages out.
- As a best practice, do not configure MAC authentication guest VLANs or critical VLANs. The VLANs might fail to work correctly when both EAD assistant and MAC authentication are configured on the device.
- As a best practice, do not configure the Web authentication or IP source guard feature. These features might fail to work correctly when both EAD assistant and MAC authentication are configured on the device.
- If the MAC address of a user has been marked as a silent MAC address before you enable EAD assistant, packets from the user can trigger 802.1X or MAC authentication only after the quiet timer expires.
- As from Release 6331, the **dot1x ead-assistant permit authentication-escape** command is added to remove the MAC authentication critical VLAN malfunction issue when EAD assistant is enabled. This command enables the device to remove the EAD entries of users before it assigns the users to MAC authentication critical VLANs.

To redirect the HTTPS requests of 802.1X users, you must execute the **dot1x ead-assistant url** command. By default, the device listens to port 6654 for HTTPS requests to be redirected. To change the redirect listening port number, see configuring HTTP redirect in *Layer 3—IP Services Configuration Guide*.

Examples

Enable the EAD assistant feature.

```
<Sysname> system-view
[Sysname] dot1x ead-assistant enable
```

Related commands

display dot1x

dot1x ead-assistant free-ip

dot1x ead-assistant url

http-redirect https-port (*Layer 3—IP Services Command Reference*)

dot1x ead-assistant free-ip

Use **dot1x ead-assistant free-ip** to configure a free IP.

Use **undo dot1x ead-assistant free-ip** to remove the specified or all free IP addresses.

Syntax

dot1x ead-assistant free-ip *ip-address* { *mask-address* | *mask-length* }

undo dot1x ead-assistant free-ip { *ip-address* { *mask-address* | *mask-length* } | **all** }

Default

No free IPs exist. Users cannot access any segments before they pass 802.1X authentication.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies a freely accessible IP address segment, also called a free IP.

mask: Specifies an IP address mask.

mask-length: Specifies IP address mask length in the range of 1 to 32.

all: Removes all free IP addresses.

Usage guidelines

With EAD assistant enabled on the device, unauthenticated 802.1X users can access the network resources in the free IP segments before they pass 802.1X authentication.

Execute this command multiple times to configure multiple free IPs.

Examples

Configure 192.168.1.1/16 as a free IP.

```
<Sysname> system-view
[Sysname] dot1x ead-assistant free-ip 192.168.1.1 255.255.0.0
```

Related commands

display dot1x

dot1x ead-assistant enable

dot1x ead-assistant url

dot1x ead-assistant permit authentication-escape

Use **dot1x ead-assistant permit authentication-escape** to enable support for 802.1X Auth-Fail and critical VLANs and MAC authentication critical VLANs when 802.1X EAD assistant is enabled.

Use **undo dot1x ead-assistant permit authentication-escape** to restore the default.

Syntax

dot1x ead-assistant permit authentication-escape

undo dot1x ead-assistant permit authentication-escape

Default

802.1X Auth-Fail and critical VLANs and MAC authentication critical VLANs cannot take effect when 802.1X EAD assistant is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command is supported only in Release 6331 and later.

This command enables the device to remove the EAD entries of users before it assigns the users to 802.1X Auth-Fail or critical VLANs or MAC authentication critical VLANs.

Examples

Enable support for 802.1X Auth-Fail and critical VLANs and MAC authentication critical VLANs when 802.1X EAD assistant is enabled.

```
<Sysname> system-view
[Sysname] dot1x ead-assistant permit authentication-escape
```

Related commands

dot1x ead-assistant enable

dot1x ead-assistant url

Use **dot1x ead-assistant url** to configure a redirect URL for EAD assistant.

Use **undo dot1x ead-assistant url** to restore the default.

Syntax

dot1x ead-assistant url *url-string*

undo dot1x ead-assistant url

Default

No redirect URL exists for EAD assistant.

Views

System view

Predefined user roles

network-admin

Parameters

url-string: Specifies the redirect URL, a case-sensitive string of 1 to 256 characters in the format http://*string* or https://*string*. If the specified URL does not start with http:// or https://, the device prefixes the specified URL with http://. Because the URL string can contain question marks (?), you cannot obtain help information by entering a question mark at the position of this argument.

Usage guidelines

When an unauthenticated user uses a Web browser to access any network other than the free IP, the device redirects the HTTP or HTTPS requests of the user to the redirect URL.

The redirect URL must be on the free IP subnet.

If you execute this command multiple times, the most recent configuration takes effect.

By default, the device listens to port 6654 for HTTPS requests to be redirected. To change the redirect listening port number, see configuring HTTP redirect in *Layer 3—IP Services Configuration Guide*.

Examples

Configure the redirect URL as http://test.com.

```
<Sysname> system-view
[Sysname] dot1x ead-assistant url http://test.com
```

Related commands

display dot1x

dot1x ead-assistant enable

dot1x ead-assistant free-ip

http-redirect https-port (*Layer 3—IP Services Command Reference*)

dot1x eap-tls-fragment to-server

Use **dot1x eap-tls-fragment to-server** to enable 802.1X EAP-TLS fragmentation and set the maximum EAP-TLS fragment size.

Use **undo dot1x eap-tls-fragment to-server** to restore the default.

Syntax

dot1x eap-tls-fragment to-server *eap-tls-max-length*

undo dot1x eap-tls-fragment to-server

Default

EAP-TLS messages are not fragmented.

Views

System view

Predefined user roles

network-admin

Parameters

eap-tls-max-length: Sets the maximum EAP-TLS fragment size in bytes. The value range is 100 to 1500.

Usage guidelines

802.1X EAP-TLS fragmentation takes effect only when EAP relay mode is used.

When the device uses EAP-TLS authentication method in EAP relay mode, the RADIUS packets might exceed the maximum packet size supported by the RADIUS server. This situation typically occurs when long EAP-TLS messages are encapsulated in the EAP-Message attribute of the RADIUS packet sent to the RADIUS server.

To avoid authentication failures caused by oversized packets, fragment the EAP-TLS messages depending on the maximum RADIUS packet size supported by the remote RADIUS server.

For example, the maximum packet length allowed by the server is 1200 bytes and the length of a RADIUS packet (excluding the EAP-Message attribute) is 800 bytes. To make sure the maximum length of a RADIUS packet does not exceed 1200 bytes, you must set the maximum length of an EAP-TLS fragment to a value less than 400 bytes.

Examples

Set the maximum EAP-TLS fragment size to 400 bytes.

```
<Sysname> system-view
[Sysname] dot1x eap-tls-fragment to-server 400
```

Related commands

display dot1x

dot1x authentication-method

dot1x eapol untag

Use **dot1x eapol untag** to enable the device to remove the VLAN tags of all 802.1X protocol packets sent out of a port to 802.1X clients.

Use **undo dot1x eapol untag** to restore the default.

Syntax

dot1x eapol untag

undo dot1x eapol untag

Default

Whether the device removes the VLAN tags of all 802.1X protocol packets sent out of a port to 802.1X clients depends on the configuration in the VLAN module.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

CAUTION:

This command removes the VLAN tags of all 802.1X protocol packets sent out of the port to 802.1X clients. Do not use this command if VLAN-aware 802.1X clients are attached to the port. As a best practice, use this command only in the scenario described in the command usage guidelines.

This command operates on a hybrid port to have it send 802.1X protocol packets with their VLAN tags removed, regardless of whether the port is a tagged or untagged member of a VLAN.

Use this command if the 802.1X-enabled hybrid port is a tagged member of its PVID and the attached 802.1X clients cannot recognize VLAN-tagged 802.1X protocol packets.

Examples

Enable the device to remove the VLAN tags of all 802.1X protocol packets sent out of GigabitEthernet 1/0/1 to 802.1X clients.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x eapol untag
```

Related commands

display dot1x

dot1x guest-vlan

Use **dot1x guest-vlan** to configure an 802.1X guest VLAN on a port.

Use **undo dot1x guest-vlan** to restore the default.

Syntax

dot1x guest-vlan *guest-vlan-id*

undo dot1x guest-vlan

Default

No 802.1X guest VLAN exists on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

guest-vlan-id: Specifies the ID of the 802.1X guest VLAN. The value range for the VLAN ID is 1 to 4094. Make sure the VLAN has been created.

Usage guidelines

An 802.1X guest VLAN accommodates users that have not performed 802.1X authentication. In the guest VLAN, users can access a limited set of network resources, such as a software server, to download anti-virus software and system patches.

To delete a VLAN that has been configured as a guest VLAN, you must use the **undo dot1x guest-vlan** command first.

Examples

Specify VLAN 100 as the 802.1X guest VLAN on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x guest-vlan 100
```

Related commands

display dot1x

dot1x guest-vlan-delay

Use **dot1x guest-vlan-delay** to enable 802.1X guest VLAN assignment delay on a port.

Use **undo dot1x guest-vlan-delay** to disable the specified 802.1X guest VLAN assignment delay on a port.

Syntax

dot1x guest-vlan-delay { **eapol** | **new-mac** }

undo dot1x guest-vlan-delay [**eapol** | **new-mac**]

Default

802.1X guest VLAN assignment delay is disabled on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

eapol: Specifies EAPOL-triggered 802.1X guest VLAN assignment delay. This keyword takes effect if 802.1X authentication is triggered by EAPOL-Start packets.

new-mac: Specifies new MAC-triggered 802.1X guest VLAN assignment delay. This keyword takes effect if 802.1X authentication is triggered by packets from unknown MAC addresses.

Usage guidelines

This command enables the device to delay assigning an 802.1X-enabled port to the 802.1X guest VLAN when 802.1X authentication is triggered on the port.

To use this feature, the 802.1X-enabled port must perform MAC-based access control.

When 802.1X authentication is triggered on a port, the device performs the following operations:

1. Sends a unicast EAP-Request/Identity packet to the MAC address that triggers the authentication.
2. Retransmits the packet if no response has been received within the username request timeout interval set by using the **dot1x timer tx-period** command.
3. Assigns the port to the 802.1X guest VLAN after the maximum number of request attempts set by using the **dot1x retry** command is reached.

If you use the **undo** command without any keyword, the command disables both EAPOL-triggered and new MAC-triggered 802.1X guest VLAN assignment delay on a port.

Examples

Enable EAPOL-triggered 802.1X guest VLAN assignment delay on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x guest-vlan-delay eapol
```

Related commands

display dot1x

dot1x guest-vlan

dot1x retry

dot1x timer tx-period

dot1x handshake

Use **dot1x handshake** to enable the online user handshake feature.

Use **undo dot1x handshake** to disable the online user handshake feature.

Syntax

dot1x handshake

undo dot1x handshake

Default

The online user handshake feature is enabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

The online user handshake feature enables the device to periodically send EAP-Request/Identity packets to the client for verifying the connectivity status of online 802.1X users. The device sets a user to the offline state if it does not receive an EAP-Response/Identity packet from the user after making the maximum attempts within the handshake period. To set the handshake timer, use the **dot1x timer handshake-period** command. To set the maximum handshake attempts, use the **dot1x retry** command.

Examples

Enable the online user handshake feature on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x handshake
```

Related commands

display dot1x

dot1x timer handshake-period

dot1x retry

dot1x handshake reply enable

Use **dot1x handshake reply enable** to enable the 802.1X online user handshake reply feature.

Use **undo dot1x handshake reply enable** to disable the 802.1X online user handshake reply feature.

Syntax

dot1x handshake reply enable

undo dot1x handshake reply enable

Default

The 802.1X online user handshake reply feature is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

This command enables the device to reply to 802.1X clients' EAP-Response/Identity packets with EAP-Success packets during the online handshake process.

Use this command only if 802.1X clients will go offline without receiving EAP-Success packets from the device.

Examples

Enable the 802.1X online user handshake reply feature on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x handshake reply enable
```

Related commands

dot1x handshake

dot1x handshake secure

Use **dot1x handshake secure** to enable the online user handshake security feature.

Use **undo dot1x handshake secure** to disable the online user handshake security feature.

Syntax

dot1x handshake secure

undo dot1x handshake secure

Default

The online user handshake security feature is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

The online user handshake security feature enables the device to prevent users from using illegal client software.

The feature is implemented based on the online user handshake feature. To bring the security function into effect, make sure the online user handshake feature is enabled.

The online user handshake security feature takes effect only on the network where the iNode client and IMC server are used.

Examples

Enable the online user handshake security feature on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x handshake secure
```

Related commands

display dot1x

dot1x handshake

dot1x mac-binding

Use **dot1x mac-binding** to add an 802.1X MAC address binding entry.

Use **undo dot1x mac-binding** to delete the specified 802.1X MAC address binding entries.

Syntax

dot1x mac-binding *mac-address*

undo dot1x mac-binding { *mac-address* | **all** }

Default

No 802.1X MAC address binding entries exist on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

mac-address: Specifies a MAC address in the format of H-H-H, excluding broadcast, multicast, and all-zero MAC addresses.

all: Specifies all MAC addresses that are bound to a port.

Usage guidelines

This command takes effect only when the 802.1X MAC address binding feature takes effect.

802.1X MAC address binding entries, both manually added and automatically generated, never age out. They can survive a user logoff or a device reboot. To delete an entry, use the **undo dot1x mac-binding** *mac-address* command. An 802.1X MAC address binding entry cannot be deleted when the user in the entry is online.

After the number of 802.1X MAC address binding entries reaches the upper limit of concurrent 802.1X users (set by using the **dot1x max-user** command), the following restrictions exist:

- Users not in the binding entries will fail authentication even after users in the binding entries go offline.
- New 802.1X MAC address binding entries are not allowed.

Examples

Add an 802.1X MAC address binding entry on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x mac-binding 000a-eb29-75f1
```

Related commands

dot1x

dot1x mac-binding enable

dot1x port-method

dot1x mac-binding enable

Use **dot1x mac-binding enable** to enable the 802.1X MAC address binding feature.

Use **undo dot1x mac-binding enable** to disable the 802.1X MAC address binding feature.

Syntax

dot1x mac-binding enable

undo dot1x mac-binding enable

Default

The 802.1X MAC address binding feature is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only on a port that performs MAC-based access control.

The 802.1X MAC address binding feature automatically binds MAC addresses of authenticated 802.1X users to the users' access port and generates 802.1X MAC address binding entries.

802.1X MAC address binding entries, both automatically generated and manually added, never age out. They can survive a user logoff or a device reboot. To delete an entry, use the **undo dot1x mac-binding** *mac-address* command. An 802.1X MAC address binding entry cannot be deleted when the user in the entry is online.

After the number of 802.1X MAC address binding entries reaches the upper limit of concurrent 802.1X users (set by using the **dot1x max-user** command), the following restrictions exist:

- Users not in the binding entries will fail authentication even after users in the binding entries go offline.
- New 802.1X MAC address binding entries are not allowed.

Examples

Enable 802.1X MAC address binding on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x mac-binding enable
```

Related commands

dot1x

dot1x mac-binding

dot1x port-method

dot1x mandatory-domain

Use **dot1x mandatory-domain** to specify a mandatory 802.1X authentication domain on a port.

Use **undo dot1x mandatory-domain** to restore the default.

Syntax

dot1x mandatory-domain *domain-name*

undo dot1x mandatory-domain

Default

No mandatory 802.1X authentication domain is specified on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

domain-name: Specifies the ISP domain name, a case-insensitive string of 1 to 255 characters.

Usage guidelines

When the system authenticates an 802.1X user trying to access a port, it selects an authentication domain in the following order:

1. Mandatory domain.
2. ISP domain specified in the username.
3. Default ISP domain.

Examples

Specify **my-domain** as the mandatory authentication domain for 802.1X users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x mandatory-domain my-domain
```

Related commands

display dot1x

dot1x max-user

Use **dot1x max-user** to set the maximum number of concurrent 802.1X users on a port.

Use **undo dot1x max-user** to restore the default.

Syntax

dot1x max-user *max-number*

undo dot1x max-user

Default

A port allows a maximum of 4294967295 concurrent 802.1X users.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

max-number: Specifies the maximum number of concurrent 802.1X users on a port. The value range is 1 to 4294967295.

Usage guidelines

Set the maximum number of concurrent 802.1X users on a port to prevent the system resources from being overused. When the maximum number is reached, the port denies subsequent 802.1X users.

Examples

Set the maximum number of concurrent 802.1X users to 32 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x max-user 32
```

Related commands

display dot1x

dot1x multicast-trigger

Use **dot1x multicast-trigger** to enable the 802.1X multicast trigger feature.

Use **undo dot1x multicast-trigger** to disable the 802.1X multicast trigger feature.

Syntax

dot1x multicast-trigger

undo dot1x multicast-trigger

Default

The 802.1X multicast trigger feature is enabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

The multicast trigger feature enables the device to act as the initiator. The device periodically multicasts EAP-Request/Identity packets out of a port to detect 802.1X clients and trigger authentication. You can use the **dot1x timer tx-period** command to set the interval for sending multicast EAP-Request/Identity packets.

Examples

Enable the multicast trigger feature on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x multicast-trigger
```

Related commands

display dot1x

dot1x timer tx-period

dot1x unicast-trigger

dot1x packet-detect enable

Use **dot1x packet-detect enable** to enable packet detection for 802.1X authentication.

Use **undo dot1x packet-detect enable** to restore the default.

NOTE:

This command is supported only in Release 6348P01 and later

Syntax

dot1x packet-detect enable

undo dot1x packet-detect enable

Default

Packet detection for 802.1X authentication is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

When packet detection for 802.1X authentication is enabled on a port, the device sends detection packets to 802.1X users connected to that port at offline detection intervals set by using the offline detection timer. If the device does not receive a response from a user after it has made the maximum packet transmission attempts within an offline detection interval, it logs off that user and requests the RADIUS server to stop accounting for the user.

When packet detection for 802.1X authentication and 802.1X offline detection are both enabled, the device processes an 802.1X user as follows:

- If 802.1X offline detection determines that a user is online, the device does not send detection packets to that user.
- If 802.1X offline detection determines that a user is offline, the device does not immediately logs off that user. Instead, the device sends a detection packet to that user. It will log off that user if it does not receive a response from that user after it has made the maximum packet transmission attempts within an offline detection interval.

To ensure that the device is aware of user IP address changes, enable ARP snooping and ND snooping in conjunction with packet detection for 802.1X authentication. If you do not enable ARP snooping or ND snooping, the device is unaware of user IP address changes. As a result, the device still sends detection packets to the users' original IP addresses and falsely log off these users.

Examples

Enable packet detection for 802.1X authentication.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x packet-detect enable
```

Related commands

dot1x timer offline-detect

port-security packet-detect arp-source-ip factor

dot1x packet-detect retry

dot1x packet-detect retry

Use **dot1x packet-detect retry** to set the maximum number of attempts for sending a detection packet to an 802.1X user.

Use **undo dot1x packet-detect retry** to restore the default.

NOTE:

This command is supported only in Release 6348P01 and later

Syntax

dot1x packet-detect retry *retries*

undo dot1x packet-detect retry

Default

The device sends a detection packet to an 802.1X user for a maximum of two times.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

retries: Sets the maximum number of attempts for sending a detection packet to an 802.1X user. The value range is 1 to 10.

Usage guidelines

When packet detection for 802.1X authentication is enabled on a port, the device sends detection packets to 802.1X users connected to that port at offline detection intervals set by using the offline detection timer. If the device does not receive a response from a user after it has made the maximum packet transmission attempts within an offline detection interval, it logs off that user and requests the RADIUS server to stop accounting for the user.

If the device fails to send a detection packet to an 802.1X user because it does not obtain the IP address of that user when that user just comes online, the device still decreases the maximum packet transmission attempts by 1. To prevent an 802.1X user from being logged off because the device does not obtain the IP address of that user when that user just comes online, the device increases the maximum number of packet transmission attempts by 10 on the basis of the original configuration.

Examples

Set the maximum number of attempts to 8 for sending a detection packet to an 802.1X user.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x packet-detect retry 8
```

Related commands

dot1x packet-detect enable

dot1x port-control

Use **dot1x port-control** to set the authorization state for the port.

Use **undo dot1x port-control** to restore the default.

Syntax

dot1x port-control { **authorized-force** | **auto** | **unauthorized-force** }

undo dot1x port-control

Default

The default port authorization state is **auto**.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

authorized-force: Places the port in authorized state, enabling users on the port to access the network without authentication.

auto: Places the port initially in unauthorized state to allow only EAPOL packets to pass, and places the port in authorized state after a user passes authentication. You can use this option in most scenarios.

unauthorized-force: Places the port in unauthorized state, denying any access requests from users on the port.

Usage guidelines

You can use this command to set the port authorization state to determine whether a client is granted access to the network.

Examples

Set the authorization state of GigabitEthernet 1/0/1 to **unauthorized-force**.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x port-control unauthorized-force
```

Related commands

display dot1x

dot1x port-method

Use **dot1x port-method** to specify an access control method for the port.

Use **undo dot1x port-method** to restore the default.

Syntax

dot1x port-method { **macbased** | **portbased** }

undo dot1x port-method

Default

MAC-based access control applies.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

macbased: Uses MAC-based access control on the port to separately authenticate each user attempting to access the network. Using this method, when an authenticated user logs off, no other online users are affected.

portbased: Uses port-based access control on the port. Using this method, once an 802.1X user passes authentication on the port, any subsequent user can access the network through the port without authentication. When the authenticated user logs off, all other users are logged off.

Usage guidelines

If online 802.1X users are present on a port, changing its access control method will cause the online users to go offline.

Examples

Configure GigabitEthernet 1/0/1 to implement port-based access control.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x port-method portbased
```

Related commands

display dot1x

dot1x quiet-period

Use **dot1x quiet-period** to enable the quiet timer.

Use **undo dot1x quiet-period** to disable the quiet timer.

Syntax

dot1x quiet-period

undo dot1x quiet-period

Default

The quiet timer is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

When a client fails 802.1X authentication, the device must wait a period of time before it can process authentication requests from the client. You can use the **dot1x timer quiet-period** command to set the quiet timer.

Examples

Enable the quiet timer and set the quiet timer to 100 seconds.

```
<Sysname> system-view
[Sysname] dot1x quiet-period
[Sysname] dot1x timer quiet-period 100
```

Related commands

display dot1x

dot1x timer

dot1x re-authenticate

Use **dot1x re-authenticate** to enable the 802.1X periodic reauthentication feature.

Use **undo dot1x re-authenticate** to disable the 802.1X periodic reauthentication feature.

Syntax

dot1x re-authenticate

undo dot1x re-authenticate

Default

The 802.1X periodic reauthentication feature is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

Periodic reauthentication enables the access device to periodically authenticate online 802.1X users on a port. This feature tracks the connection status of online users and updates the authorization attributes assigned by the server, such as the ACL and VLAN.

You can use the **dot1x timer reauth-period** command to configure the interval for reauthentication.

If periodic reauthentication is triggered for a user while that user is waiting for online synchronization, the system performs online synchronization and does not perform reauthentication for the user.

Examples

Enable the 802.1X periodic reauthentication feature on GigabitEthernet 1/0/1, and set the periodic reauthentication interval to 1800 seconds.

```
<Sysname> system-view
[Sysname] dot1x timer reauth-period 1800
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x re-authenticate
```

Related commands

display dot1x

dot1x server-recovery online-user-sync

dot1x timer

dot1x re-authenticate manual

Use **dot1x re-authenticate manual** to manually reauthenticate all online 802.1X users on a port.

Syntax

dot1x re-authenticate manual

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

After this command is executed, this device reauthenticates all online 802.1X users on a port. The command takes effect regardless of the server-assigned reauthentication attribute and the periodic reauthentication feature.

Examples

Manually reauthenticate all online 802.1X users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x re-authenticate manual
```

Related commands

dot1x re-authenticate

dot1x re-authenticate server-unreachable keep-online

Use **dot1x re-authenticate server-unreachable keep-online** to enable the keep-online feature on a port.

Use **undo dot1x re-authenticate server-unreachable** to restore the default.

Syntax

dot1x re-authenticate server-unreachable keep-online

undo dot1x re-authenticate server-unreachable

Default

The keep-online feature is disabled on a port. The device logs off online 802.1X authenticated users if no server is reachable for 802.1X reauthentication.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

This feature keeps authenticated 802.1X users online when no server is reachable for 802.1X reauthentication.

Examples

Enable the keep-online feature on GigabitEthernet 1/0/1 for 802.1X reauthentication.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x re-authenticate server-unreachable keep-online
```

Related commands

display dot1x

dot1x re-authenticate

dot1x retry

Use **dot1x retry** to set the maximum number of attempts for sending an authentication request to a client.

Use **undo dot1x retry** to restore the default.

Syntax

dot1x retry *retries*

undo dot1x retry

Default

A maximum of two attempts are made to send an authentication request to a client.

Views

System view

Predefined user roles

network-admin

Parameters

retries: Specifies the maximum number of attempts for sending an authentication request to a client. The value range is 1 to 10.

Usage guidelines

The access device retransmits an authentication request to a client in any of the following situations:

- The device does not receive any responses from the client within the username request timeout interval. The timer is set by using the **dot1x timer tx-period** *tx-period-value* command for the EAP-Request/Identity packet.
- The device does not receive any responses from the client within the client timeout interval. The timer is set by using the **dot1x timer supp-timeout** *supp-timeout-value* command for the EAP-Request/MD5-Challenge packet.

The access device stops retransmitting the request, if it has made the maximum number of request transmission attempts but still received no response.

Examples

Set the maximum number of attempts to 9 for sending an authentication request to a client.

```
<Sysname> system-view
[Sysname] dot1x retry 9
```

Related commands

display dot1x

dot1x timer

dot1x server-recovery online-user-sync

Use **dot1x server-recovery online-user-sync** to enable 802.1X online user synchronization.

Use **undo dot1x server-recovery online-user-sync** to disable 802.1X online user synchronization.

Syntax

dot1x server-recovery online-user-sync

undo dot1x server-recovery online-user-sync

Default

802.1X online user synchronization is disabled. The device does not synchronize online 802.1X user information on a port with a RADIUS server after the RADIUS server recovers from the unreachable state.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

IMPORTANT:

This command takes effect only when the device uses an IMC RADIUS server to authenticate 802.1X users.

To ensure that the RADIUS server maintains the same online 802.1X user information as the device after the server state changes from unreachable to reachable, use this feature.

This feature synchronizes online 802.1X user information between the device and the RADIUS server when the RADIUS server state is detected having changed from unreachable to reachable.

When synchronizing online 802.1X user information on a port with the RADIUS server, the device initiates 802.1X authentication in turn for each authenticated online 802.1X user to the RADIUS server.

If synchronization fails for an online user, the device logs off that user unless the failure occurs because the server has become unreachable again.

The amount of time required to complete online user synchronization increases as the number of online users grows. This might result in an increased delay for new 802.1X users and users in the critical VLAN to authenticate or reauthenticate to the RADIUS server and come online.

To have this feature take effect, you must use it in conjunction with the RADIUS server status detection feature, which is configurable with the **radius-server test-profile** command. When you configure this feature, make sure the detection interval is shorter than the RADIUS server quiet timer configured by using the **timer quiet** command in RADIUS scheme view. The server state changes to active on expiration of the quiet timer regardless of its actual reachability. Setting a shorter detection interval than the quiet timer prevents the RADIUS server status detection feature from falsely reporting the server reachability.

For more information about the RADIUS server status detection feature, see AAA configuration in *Security Configuration Guide*.

Examples

Enable 802.1X online user synchronization on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x server-recovery online-user-sync
```

Related commands

display dot1x

radius-server test-profile

timer quiet (RADIUS scheme view)

dot1x timer

Use **dot1x timer** to set an 802.1X timer.

Use **undo dot1x timer** to restore the default of an 802.1X timer.

Syntax

dot1x timer { **ead-timeout** *ead-timeout-value* | **handshake-period** *handshake-period-value* | **quiet-period** *quiet-period-value* | **reauth-period** *reauth-period-value* | **server-timeout** *server-timeout-value* | **supp-timeout** *supp-timeout-value* | **tx-period** *tx-period-value* | **user-aging** { **auth-fail-vlan** | **critical-vlan** | **guest-vlan** } *aging-time-value* }

undo dot1x timer { **ead-timeout** | **handshake-period** | **quiet-period** | **reauth-period** | **server-timeout** | **supp-timeout** | **tx-period** | **user-aging** { **auth-fail-vlan** | **critical-vlan** | **guest-vlan** } }

Default

The following 802.1X timers apply:

- EAD rule timer: 30 minutes.
- Handshake timer: 15 seconds.
- Quiet timer: 60 seconds.
- Periodic reauthentication timer: 3600 seconds.
- Server timeout timer: 100 seconds.
- Client timeout timer: 30 seconds.
- Username request timeout timer: 30 seconds.
- User aging timers for all applicable types of 802.1X VLANs: 1000 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

ead-timeout *ead-timeout-value*: Sets the EAD rule timer in minutes. The value range for the *ead-timeout-value* argument is 1 to 1440.

handshake-period *handshake-period-value*: Sets the handshake timer in seconds. The value range for the *handshake-period-value* argument is 5 to 1024.

quiet-period *quiet-period-value*: Sets the quiet timer in seconds. The value range for the *quiet-period-value* argument is 10 to 120.

reauth-period *reauth-period-value*: Sets the periodic reauthentication timer in seconds. The value range for the *reauth-period-value* argument is 60 to 7200 prior to Release 6342. As from Release 6343P08, the value range for this argument is 60 to 86400.

server-timeout *server-timeout-value*: Sets the server timeout timer in seconds. The value range for the *server-timeout-value* argument is 100 to 300.

supp-timeout *supp-timeout-value*: Sets the client timeout timer in seconds. The value range for the *supp-timeout-value* argument is 1 to 120.

tx-period *tx-period-value*: Sets the username request timeout timer in seconds. The value range for the *tx-period-value* argument is 1 to 120.

user-aging: Sets the user aging timer for a type of 802.1X VLAN.

auth-fail-vlan: Specifies 802.1X Auth-Fail VLANs.

critical-vlan: Specifies 802.1X critical VLANs.

guest-vlan: Specifies 802.1X guest VLANs.

aging-time-value: Sets the user aging timer. The value range is 60 to 2147483647 seconds.

Usage guidelines

In most cases, the default settings are sufficient. You can edit the timers, depending on the network conditions.

- In a low-speed network, increase the client timeout timer.
- In a vulnerable network, set the quiet timer to a high value.
- In a high-performance network with quick authentication response, set the quiet timer to a low value.
- In a network with authentication servers of different performance, adjust the server timeout timer.

The network device uses the following 802.1X timers:

- **EAD rule timer (ead-timeout)**—Sets the lifetime of each EAD rule. When the timer expires or the user passes authentication, the rule is removed. If users fail to download the EAD client or fail to pass authentication before the timer expires, they must reconnect to the network to access the free IP.
- **Handshake timer (handshake-period)**—Sets the interval at which the access device sends client handshake requests to check the online status of a client that has passed authentication. If the device does not receive a response after sending the maximum number of handshake requests, it considers that the client has logged off.
- **Quiet timer (quiet-period)**—Starts when a client fails authentication. The access device must wait the time period before it can process the authentication attempts from the client.
- **Periodic reauthentication timer (reauth-period)**—Sets the interval at which the network device periodically reauthenticates online 802.1X users. To enable 802.1X periodic reauthentication on a port, use the **dot1x re-authenticate** command.
- **Server timeout timer (server-timeout)**—Starts when the access device sends a RADIUS Access-Request packet to the authentication server. If no response is received when this timer expires, the 802.1X authentication fails.

  To avoid forced logoff before the server timeout timer expires, set the server timeout timer to a value that is lower than or equal to the product of the following values:

  - The maximum number of RADIUS packet transmission attempts set by using the **retry** command in RADIUS scheme view.
  - The RADIUS server response timeout timer set by using the **timer response-timeout** command in RADIUS scheme view.

  For information about setting the maximum number of RADIUS packet transmission attempts and the RADIUS server response timeout timer, see AAA configuration in *Security Configuration Guide*.
- **Client timeout timer (supp-timeout)**—Starts when the access device sends an EAP-Request/MD5-Challenge packet to a client. If no response is received when this timer expires, the access device retransmits the request to the client.
- **Username request timeout timer (tx-period)**—Starts when the device sends an EAP-Request/Identity packet to a client in response to an authentication request. If the device does not receive a response before this timer expires, it retransmits the request. The timer also sets the interval at which the network device sends multicast EAP-Request/Identity packets to detect clients that cannot actively request authentication.

- **User aging timer (`user-aging`)**—Sets the user aging timer for a type of 802.1X VLAN.

  If you enable 802.1X unauthenticated user aging, you can set a user aging timer for Auth-Fail, critical, or guest VLANs. The user aging timer for a type of 802.1X VLAN determines how long a user can stay in that type of VLAN.

  For more information about how user aging operates, see the usage guidelines for the **`dot1x unauthenticated-user aging enable`** command.

  Do not set a user aging timer to a multiple of the username request timeout timer (the **`dot1x timer tx-period`** command). If you do so, the aging timer will not take effect.

The change to the periodic reauthentication timer applies to the users that have been online only after the old timer expires. Other timer changes take effect immediately on the device.

Examples

Set the server timeout timer to 150 seconds.

```
<Sysname> system-view
[Sysname] dot1x timer server-timeout 150
```

Related commands

`display dot1x`

`dot1x unauthenticated-user aging enable`

`retry`

`timer response-timeout` (RADIUS scheme view)

dot1x timer reauth-period

Use **`dot1x timer reauth-period`** to set the 802.1X periodic reauthentication timer on a port.

Use **`undo dot1x timer reauth-period`** to restore the default.

Syntax

`dot1x timer reauth-period` *`reauth-period-value`*

`undo dot1x timer reauth-period`

Default

No 802.1X periodic reauthentication timer is configured on a port. The port uses the global 802.1X periodic reauthentication timer.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

`reauth-period-value`: Sets the 802.1X periodic reauthentication timer in seconds. The value range for the *`reauth-period-value`* argument is 60 to 7200 prior to Release 6342. As from Release 6343P08, the value range for this argument is 60 to 86400..

Usage guidelines

The device reauthenticates online 802.1X users on a port at the specified periodic reauthentication interval when the port is enabled with periodic reauthentication. To enable periodic reauthentication on a port, use the **`dot1x re-authenticate`** command.

A change to the periodic reauthentication timer applies to online users only after the old timer expires.

The device selects a periodic reauthentication timer for 802.1X reauthentication in the following order:

1. Server-assigned reauthentication timer.
2. Port-specific reauthentication timer.
3. Global reauthentication timer.
4. Default reauthentication timer.

Examples

Set the 802.1X periodic reauthentication timer to 60 seconds on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x timer reauth-period 60
```

Related commands

dot1x timer

dot1x unauthenticated-user aging enable

Use **dot1x unauthenticated-user aging enable** to 802.1X unauthenticated user aging.

Use **undo dot1x unauthenticated-user aging enable** to disable 802.1X unauthenticated user aging.

Syntax

dot1x unauthenticated-user aging enable

undo dot1x unauthenticated-user aging enable

Default

User aging is enabled for 802.1X users that have not been authenticated or have not passed authentication.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

802.1X unauthenticated user aging applies to users added to 802.1X guest, critical, or Auth-Fail VLANs because they have not been authenticated or have failed authentication.

When a user in one of those VLANs ages out, the device removes the user from the VLAN and deletes the MAC address entry for the user from the access port.

The 802.1X user aging mechanism on a port depends on its access control mode.

- If the port uses port-based access control, a user aging timer starts when the port is assigned to the critical or Auth-Fail VLAN. When the aging timer expires, the port is removed from the VLAN and all MAC address entries for users in the VLAN are also removed.
- If the port uses MAC-based access control, a user aging timer starts for each 802.1X user when they are assigned to the Auth-Fail, critical, or guest VLAN. When the aging timer for a user expires, the device removes that user from the VLAN.

For users in one of those VLANs on one port to be authenticated successfully and come online on another port, enable this feature. In any other scenarios, disable this feature as a best practice.

The removed users will be unable to access any network resources until after another authentication is triggered.

Examples

Disable 802.1X user aging on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo dot1x unauthenticated-user aging enable
```

Related commands

dot1x timer

dot1x unicast-trigger

Use **dot1x unicast-trigger** to enable the 802.1X unicast trigger feature.

Use **undo dot1x unicast-trigger** to disable the 802.1X unicast trigger feature.

Syntax

dot1x unicast-trigger

undo dot1x unicast-trigger

Default

The 802.1X unicast trigger feature is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

The unicast trigger feature enables the access device to initiate 802.1X authentication when the device receives a data frame from an unknown source MAC address. The device sends a unicast EAP-Request/Identity packet to the unknown source MAC address. It will retransmit the packet if it does not receive any responses within a period of time (set by using the **dot1x timer tx-period** command). This process continues until the maximum number of request attempts (set by using the **dot1x retry** command) is reached.

As a best practice, do not use the unicast trigger on a port that performs port-based access control. If you do so, users on the port might fail to come online correctly.

Examples

Enable the unicast trigger feature on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x unicast-trigger
```

Related commands

display dot1x

dot1x multicast-trigger

dot1x port-method

dot1x retry

dot1x timer

dot1x user-ip freeze

Use **dot1x user-ip freeze** to enable 802.1X user IP freezing.

Use **undo dot1x user-ip freeze** to disable 802.1X user IP freezing.

Syntax

dot1x user-ip freeze

undo dot1x user-ip freeze

Default

802.1X user IP freezing is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

This command prevents 802.1X-generated IPSG bindings from being updated because of user IP changes. For information about IP source guard commands, see "IP source guard commands."

Examples

Enable 802.1X user IP freezing on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x user-ip freeze
```

reset dot1x access-user

Use **reset dot1x access-user** to log off 802.1X users.

Syntax

reset dot1x access-user [**interface** *interface-type interface-number* | **mac** *mac-address* | **username** *username* | **vlan** *vlan-id*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

mac *mac-address*: Specifies an 802.1X user by its MAC address. The *mac-address* argument is in the format of H-H-H.

username *username*: Specifies an 802.1X user by its name. The *username* argument is a case-sensitive string of 1 to 253 characters.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

This command is supported only in Release 6318P01 and later.

Use this command to log off the specified 802.1X users and clear information about these users from the device. These users must perform 802.1X authentication to come online again.

With a VLAN specified, this command logs off the following 802.1X users:

- Users that have passed 802.1X authentication and have been assigned the specified VLAN as the authorization VLAN by the server.
- Users that stay in the specified VLAN after they have passed 802.1X authentication, because they have not been assigned an authorization VLAN yet.
- Users that are performing 802.1X authentication in the specified VLAN.

To identify the VLAN in which a user is staying, use the **display mac-address** command.

If you do not specify any parameters, the **reset dot1x access-user** command logs off all 802.1X users on the device.

Examples

Log off all 802.1X users on GigabitEthernet 1/0/1.

```
<Sysname> reset dot1x access-user interface gigabitethernet 1/0/1
```

Related commands

display dot1x connection

reset dot1x guest-vlan

Use **reset dot1x guest-vlan** to remove users from the 802.1X guest VLAN on a port.

Syntax

reset dot1x guest-vlan interface *interface-type interface-number* [**mac-address** *mac-address*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

mac-address *mac-address*: Specifies the MAC address of an 802.1X user in the guest VLAN. If you do not specify this option, the command removes all 802.1X users from the 802.1X guest VLAN on the port.

Examples

Remove the 802.1X user with MAC address 1-1-1 from the 802.1X guest VLAN on GigabitEthernet 1/0/1.

```
<Sysname> reset dot1x guest-vlan interface gigabitethernet 1/0/1 mac-address 1-1-1
```

Related commands

dot1x guest-vlan

reset dot1x statistics

Use **reset dot1x statistics** to clear 802.1X statistics.

Syntax

reset dot1x statistics [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify a port, this command clears 802.1X statistics on all ports.

Examples

Clear 802.1X statistics on GigabitEthernet 1/0/1.

```
<Sysname> reset dot1x statistics interface gigabitethernet 1/0/1
```

Related commands

display dot1x

Contents

MAC authentication commands

display mac-authentication

Use **display mac-authentication** to display MAC authentication settings and statistics.

Syntax

display mac-authentication [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If the specified port is not enabled with MAC authentication, this command displays only global MAC authentication information.

Usage guidelines

If you do not specify any parameters, this command displays all MAC authentication information including the global settings, port-specific settings, MAC authentication statistics, and online user statistics.

Examples

Display all MAC authentication settings and statistics.

```
<Sysname> display mac-authentication
 Global MAC authentication parameters:
   MAC authentication                  : Enabled
   Authentication method               : PAP
   Username format                     : MAC address in lowercase(xxxxxxxxxxxx)
           Username                    : mac
           Password                    : Not configured
   MAC range accounts                  : 2
          MAC address          Mask                 Username
          2222-0000-0000       ffff-0000-0000       user1
          4444-0000-0000       ffff-0000-0000       user1

   Offline detect period               : 300 s
   Quiet period                        : 60 s
   Server timeout                      : 100 s
   Reauth period                       : 3600 s
   User aging period for critical VLAN : 1000 s
   User aging period for guest VLAN    : 1000 s
   Authentication domain               : Not configured, use default domain
 Online MAC-auth wired users           : 1

 Silent MAC users:
```

```
          MAC address       VLAN ID  From port              Port index
          0001-0000-0001    100      GE1/0/2                21

GigabitEthernet1/0/1  is link-up
  MAC authentication               : Enabled
  Carry User-IP                    : Disabled
  Authentication domain            : Not configured
  Auth-delay timer                 : Enabled
  Auth-delay period                : 60 s
  Periodic reauth                  : Enabled
      Reauth period                : 120 s
  Re-auth server-unreachable       : Logoff
  Guest VLAN                       : 100
  Guest VLAN reauthentication      : Enabled
    Guest VLAN auth-period         : 150 s
  Critical VLAN                    : Not configured
  Critical voice VLAN              : Disabled
  Host mode                        : Multiple VLAN
  Offline detection                : Enabled
  Authentication order             : Parallel
  User aging                       : Enabled
  Server-recovery online-user-sync : Enabled

  Auto-tag feature                 : Disabled
  VLAN tag configuration ignoring  : Disabled
  Max online users                 : 4294967295
  Authentication attempts          : successful 2, failed 3
  Current online users             : 1
         MAC address       Auth state
         0001-0000-0000    Authenticated
         0001-0000-0001    Unauthenticated
```

Table 1 Command output

Field	Description
MAC authentication	Whether MAC authentication is enabled globally.
Authentication method	Authentication method for MAC authentication: CHAP or PAP.
Username format	User account type: MAC-based or shared. • If MAC-based accounts are used, this field displays the format settings for the username. For example, **MAC address in lowercase(xxxxxxxxxxxx)** indicates that the MAC address is in hexadecimal notation without hyphens, and letters are in lower case. • If a shared account is used, this field displays **Fixed account**.
Username	Username for MAC authentication. • If MAC-based accounts are used, this field displays **mac**. • If a shared account is used, this field displays the username of the shared account for MAC authentication users. By default, the username is **mac**.

Field	Description
Password	Password for MAC authentication. • If the MAC address of each user is used as the password or if a shared account is used but no password is configured, this field displays **Not configured**. • If a password is configured, this field displays a string of asterisks (******).
MAC range accounts	MAC authentication user accounts specific to MAC address ranges.
MAC address	MAC address.
Mask	MAC address mask. A MAC address and a mask together specify a MAC address range.
Username	Username for the users in the MAC address range.
Offline detect period	Offline detection timer.
Quiet period	Quiet timer.
Server timeout	Server timeout timer.
Reauth period	Periodic MAC reauthentication timer in seconds.
User aging period for critical VLAN	Aging timer in seconds for users in critical VLANs.
User aging period for guest VLAN	Aging timer in seconds for users in guest VLANs.
Authentication domain	MAC authentication domain specified in system view. If no authentication domain is specified in system view, this field displays **Not configured, use default domain**.
Online MAC-auth wired users	Number of wired online MAC authentication users, including users that have passed MAC authentication and users that are performing MAC authentication.
Silent MAC users	Information about silent MAC addresses.
MAC address	Silent MAC address.
VLAN ID	ID of the VLAN to which the silent MAC address belongs.
From port	Name of the port that marks the MAC address as a silent MAC address.
Port index	Index of the port that marks the MAC address as a silent MAC address.
GigabitEthernet1/0/1 is link-up	Status of the link on GigabitEthernet 1/0/1. In this example, the link is up.
MAC authentication	Status of MAC authentication on the port: • Enabled. • Enabled (but NOT effective). This value is displayed if MAC authentication is enabled when the device does not have available ACL resources. • Disabled.
Carry User-IP	Whether user IP addresses are included in MAC authentication requests.
Authentication domain	MAC authentication domain specified for the port.
Auth-delay timer	Whether MAC authentication delay is enabled on the port.
Auth-delay period	MAC authentication delay timer.

Field	Description
Periodic reauth	Whether periodic MAC reauthentication is enabled on the port.
Reauth period	Periodic MAC reauthentication timer on the port.
Re-auth server-unreachable	Action taken when no server is reachable for MAC reauthentication: • **Logoff**—Logs off online MAC authentication users. • **Online**—Keeps MAC authenticated users online.
Guest VLAN	MAC authentication guest VLAN configured on the port. If no MAC authentication guest VLAN is configured, this field displays **Not configured**.
Guest VLAN reauthentication	This field is not supported in the current software version. Status of guest VLAN reauthentication in MAC authentication, which is **Enabled** or **Disabled**.
Guest VLAN auth-period	Authentication interval for users in the MAC authentication guest VLAN on the port.
Critical VLAN	MAC authentication critical VLAN configured on the port. If no MAC authentication critical VLAN is configured, this field displays **Not configured**.
Critical voice VLAN	Whether the MAC authentication critical voice VLAN feature is enabled on the port.
Host mode	MAC authentication VLAN mode for users moving from one VLAN to another on the port: • **Single VLAN**—Single-VLAN mode. • **Multiple VLAN**—Multi-VLAN mode.
Offline detection	Status of MAC authentication offline detection: • Enabled. • Disabled.
Authentication order	If parallel processing of MAC authentication and 802.1X authentication is disabled, this field displays **Default**. If parallel processing of MAC authentication and 802.1X authentication is enabled, this field displays **Parallel**.
User aging	Status of the aging feature for unauthenticated MAC authentication users on a port: • Enabled. • Disabled.
Server-recovery online-user-sync	Status of online user synchronization for MAC authentication on the port: • Enabled. • Disabled.
Guest VSI reauthentication	This field is not supported in the current software version. Status of guest VSI reauthentication in MAC authentication, which is **Enabled** or **Disabled**.
Auto-tag feature	This field is not supported in the current software version. Status of the authorization VLAN auto-tag feature: • **Enabled**. • **Disabled**.
VLAN tag configuration ignoring	This field is not supported in the current software version.

Field	Description
	Status of the ignore-config mode: • **Enabled**. • **Disabled**.
Max online users	Maximum number of concurrent online users allowed on the port.
Authentication attempts: successful 1, failed 0	MAC authentication statistics, including the number of successful and unsuccessful authentication attempts.
MAC address	MAC address of the online user.
Auth state	User status: • **Authenticated**—The user has passed MAC authentication. • **Unauthenticated**—The user has not passed MAC authentication.

display mac-authentication connection

Use **display mac-authentication connection** to display information about online MAC authentication users.

Syntax

display mac-authentication connection [**open**] [**interface** *interface-type interface-number* | **slot** *slot-number* | **user-mac** *mac-address* | **user-name** *user-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

open: Displays information only about MAC authentication users that use nonexistent usernames or incorrect passwords for network access in open authentication mode. If you do not specify this keyword, the command displays information about all online MAC authentication users.

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify a port, this command displays information about online MAC authentication users for all ports.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about online MAC authentication users for all member devices.

user-mac *mac-address*: Specifies an online MAC authentication user by its MAC address. The *mac-address* argument represents the MAC address of the user, in the form of H-H-H. If you do not specify an online MAC authentication user, this command displays all online MAC authentication user information.

user-name *user-name*: Specifies an online MAC authentication user by its username. The user name is a case-sensitive string of 1 to 55 characters, and it can include the domain name. If you do not specify an online MAC authentication user, this command displays all online MAC authentication user information.

Examples

Display information about all online MAC authentication users.

```
<Sysname> display mac-authentication connection
Total connections: 1
Slot ID: 0
User MAC address: 0015-e9a6-7cfe
Access interface: GigabitEthernet1/0/1
Username: ias
User access state: Successful
Authentication domain: macusers
IPv4 address: 192.168.1.1
IPv6 address: 2000:0:0:0:1:2345:6789:abcd
Initial VLAN: 1
Authorization untagged VLAN: 100
Authorization tagged VLAN: N/A
Authorization VSI: N/A
Authorization ACL number/name: 3001
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Radius-request
Session timeout period: 2 sec
Offline detection: 100 sec (server-assigned)
Packet detection:
  Max attempts: 5
  Remaining attempts: 3
  Source IPv4 address: 192.168.1.3
  Source IPv4 mask: 255.255.0.0
Online from: 2013/03/02  13:14:15
Online duration: 0h 2m 15s
```

Table 2 Command output

Field	Description
Total connections	Total number of online MAC authentication users.
User MAC address	MAC address of the user.
Access interface	Interface through which the user accesses the device.
User access state	Access state of the user: • **Successful**—The user passes MAC authentication and comes online. • **Open**—The user uses a nonexistent username or an incorrect password to come online in open authentication mode.
Authentication domain	MAC authentication domain to which the user belongs.
IPv4 address	IPv4 address of the user. If no user IPv4 address is available, this field is not displayed.
IPv6 address	IPv6 address of the user.

Field	Description
	If no user IPv6 address is available, this field is not displayed.
Initial VLAN	VLAN that holds the user before MAC authentication.
Authorization untagged VLAN	Untagged VLAN assigned to the user.
Authorization tagged VLAN	Tagged VLAN assigned to the user.
Authorization VSI	This field is not supported in the current software version. VSI assigned to the user.
Authorization ACL number/name	Number or name of the static ACL assigned to the user. If no static ACL is assigned to the user, this field displays **N/A**. If the ACL assignment fails, this field displays **(NOT effective)** next to the ACL number or name.
Authorization dynamic ACL name	This field is supported only in Release 6331 and later. Name of the dynamic ACL assigned to the user. If no dynamic ACL is assigned to the user, this field displays **N/A**. If the ACL assignment fails, this field displays **(NOT effective)** next to the ACL name.
Authorization user profile	User profile assigned to the user.
Authorization CAR	This field is not supported in the current software version. Authorization CAR attributes assigned by the server. If no authorization CAR attributes are assigned, this field displays **N/A**.
Authorization URL	Redirect URL assigned to the user.
Termination action	Action attribute assigned by the server to terminate the user session: • **Default**—Logs off the online authenticated user when the server-assigned session timeout timer expires. This attribute does not take effect when periodic MAC reauthentication is enabled and the periodic reauthentication timer is shorter than the server-assigned session timeout timer. • **Radius-request**—Reauthenticates the online user when the server-assigned session timeout timer expires, regardless of whether the periodic MAC reauthentication feature is enabled or not. If the device performs local authentication, this field displays **N/A**.
Session timeout period	Session timeout timer assigned by the server.
Offline detection	Offline detection setting for the user: • **Ignore (command-configured)**—The device does not perform offline detection for the user. The setting is configured from the CLI. • ***timer* (command-configured)**—Represents the offline detection timer. The timer is configured from the CLI, • **Ignore (server-assigned)**—The device does not perform offline detection for the user. The setting is assigned by a RADIUS server. • ***timer* (server-assigned)**—Represents the offline detection timer. The timer is assigned by a RADIUS server.
Packet detection	Information about the packet detection feature. This field is supported only in Release 6348P01 and later.
Max attempts	Maximum number of attempts for sending a detection packet to the user. This field is supported only in Release 6348P01 and later.
Remaining attempts	Remaining number of attempts for sending a detection packet to the user. The device decreases the number by 1 each time it makes an

Field	Description
	attempt to send the detection packet to the user. This field is supported only in Release 6348P01 and later.
Source IPv4 address	IP address specified for calculating the source IP address of ARP detection packets. If no IP address is specified, this field displays 0.0.0.0. This field is supported only in Release 6348P01 and later.
Source IPv4 mask	Mask specified for calculating the source IP address of ARP detection packets. If no mask is specified, this field displays 0.0.0.0. This field is supported only in Release 6348P01 and later.
Online from	Time from which the MAC authentication user came online.
Online duration	Online duration of the MAC authentication user.

display mac-authentication mac-address

Use **display mac-authentication mac-address** to display the MAC addresses of MAC authentication users in a type of MAC authentication VLAN.

Syntax

display mac-authentication mac-address { **critical-vlan** | **guest-vlan** } [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

critical-vlan: Specifies MAC authentication critical VLANs.

guest-vlan: Specifies MAC authentication guest VLANs.

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify a port, this command displays the MAC addresses of MAC authentication users in the specified type of MAC authentication VLAN on all ports.

Usage guidelines

The displayed MAC addresses and MAC address count might not include all MAC addresses if a large number of MAC authentication users are performing authentication frequently.

Examples

Display the MAC addresses of MAC authentication users in the MAC authentication guest VLANs on all ports.

```
<Sysname> display mac-authentication mac-address guest-vlan
Total MAC addresses: 10
Interface: GigabitEthernet1/0/1        Guest VLAN: 3           Aging time: N/A
MAC addresses: 8
  0800-2700-9427    0800-2700-2341    0800-2700-2324    0800-2700-2351
  0800-2700-5627    0800-2700-2251    0800-2700-8624    0800-2700-3f51
```

```
Interface: GigabitEthernet1/0/2        Guest VLAN: 5            Aging time: 30 sec
MAC addresses: 2
  0801-2700-9427    0801-2700-2341
```

Table 3 Command output

Field	Description
Total MAC addresses	Total number of MAC addresses in the specified type of VLAN on the specified port or all ports.
Interface	Access port of MAC authentication users.
Type VLAN	VLAN that contains the MAC authentication users. The *Type* argument has the following values: • Critical VLAN. • Guest VLAN.
Aging time	MAC address aging time in seconds. This field displays **N/A** if the MAC addresses do not age out.
MAC addresses	Number of matching MAC addresses on a port.
xxxx-xxxx-xxxx	MAC address.

Related commands

`mac-authentication critical vlan`

`mac-authentication guest-vlan`

mac-authentication

Use **`mac-authentication`** to enable MAC authentication globally or on a port.

Use **`undo mac-authentication`** to disable MAC authentication globally or on a port.

Syntax

`mac-authentication`

`undo mac-authentication`

Default

MAC authentication is disabled globally or on any port.

Views

System view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

To use MAC authentication on a port, you must enable the feature both globally and on the port.

Examples

Enable MAC authentication globally.

```
<Sysname> system-view
```

```
[Sysname] mac-authentication
```

Enable MAC authentication on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication
```

Related commands

display mac-authentication

mac-authentication access-user log enable

Use **mac-authentication access-user log enable** to enable MAC authentication user logging.

Use **undo mac-authentication access-user log enable** to disable MAC authentication user logging.

Syntax

mac-authentication access-user log enable [**failed-login** | **logoff** | **successful-login**] *

undo mac-authentication access-user log enable [**failed-login** | **logoff** | **successful-login**] *

Default

MAC authentication user logging is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

failed-login: Logs MAC authentication user login failures.

logoff: Logs MAC authentication user logoffs.

successful-login: Logs successful MAC authentication user logins.

Usage guidelines

To prevent excessive MAC authentication user log entries, use this feature only if you need to analyze abnormal MAC authentication user logins or logouts.

If you do not specify any parameters, this command enables all types of MAC authentication user logs.

Examples

Enable logging MAC authentication user login failures.

```
<Sysname> system-view
[Sysname] mac-authentication access-user log enable failed-login
```

Related commands

info-center source maca logfile deny (*Network Management and Monitoring Command Reference*)

mac-authentication authentication-method

Use **mac-authentication authentication-method** to specify an authentication method for MAC authentication.

Use **undo mac-authentication authentication-method** to restore the default.

Syntax

mac-authentication authentication-method { **chap** | **pap** }

undo mac-authentication authentication-method

Default

The device uses PAP for MAC authentication.

Views

System view

Predefined user roles

network-admin

Parameters

chap: Configures the access device to use the Challenge Handshake Authentication Protocol (CHAP) to communicate with the RADIUS server.

pap: Configures the access device to use the Password Authentication Protocol (PAP) to communicate with the RADIUS server.

Usage guidelines

RADIUS-based MAC authentication supports the following authentication methods:

- **PAP**—Transports usernames and passwords in plain text. The authentication method applies to scenarios that do not require high security.
- **CHAP**—Transports usernames in plain text and passwords in encrypted form over the network. CHAP is more secure than PAP.

Examples

Configure the device to use CHAP for MAC authentication.

```
<Sysname> system-view
[Sysname] mac-authentication authentication-method chap
```

Related commands

display mac-authentication

mac-authentication carry user-ip

Use **mac-authentication carry user-ip** to include user IP addresses in MAC authentication requests sent to an IMC server.

Use **undo mac-authentication carry user-ip** to restore the default.

Syntax

mac-authentication carry user-ip [**exclude-ip acl** *acl-number*]

undo mac-authentication carry user-ip

Default

A MAC authentication request does not include the user IP address.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

exclude-ip: Specifies an ACL-based filter to identify source IP addresses that can or cannot trigger MAC authentication.

acl *acl-number*: Specifies a basic ACL. The value range for the *acl-number* argument is 2000 to 2999.

Usage guidelines

IMPORTANT:

This command can only operate in conjunction with an IMC server.

To avoid IP conflicts that result from changes to static IP addresses, use this command on a port that has MAC authentication users with static IP addresses.

This command adds user IP addresses to the MAC authentication requests sent to the authentication server. When MAC authentication is triggered for a user, the device checks the user's IP address for invalidity.

- If the IP address is valid, the device sends a MAC authentication request with the IP address included.
- If the IP address is not a valid host IP address or the triggering packet does not contain an IP address, the device does not initiate MAC authentication.
- If the packet is a DHCP packet with a source IP address of 0.0.0.0, the device sends a MAC authentication request without including the IP address. In this case, the IMC server does not examine the user IP address when it performs authentication.

Upon receipt of the authentication request that includes a user's IP address, the IMC server compares the user's IP and MAC addresses with its IP-MAC mappings.

- If an exact match is found or if no match is found, the user passes MAC authentication. In the latter case, the server creates an IP-MAC mapping for the user.
- If a mapping is found for the MAC address but the IP addresses do not match, the user fails the MAC authentication.

If the user host is configured with IPv6, the device might receive packets that contain an IPv6 link-local address, which starts with fe80. MAC authentication failure or incorrect MAC-IP binding will occur if this address is used in MAC authentication. To avoid these issues, configure a basic ACL to exclude the IPv6 IP addresses that start with fe80.

When you configure the ACL, follow these guidelines:

- The specified ACL number represents an IPv4 ACL and an IPv6 ACL with the same number. For example, if the ACL number is 2000, you specify both IPv4 ACL 2000 and IPv6 ACL 2000. The IPv4 ACL and the IPv6 ACL will be used to process IPv4 packets and IPv6 packets, respectively.
- Use permit rules to identify source IP addresses that are valid for MAC authentication. Use deny rules to identify source IP addresses that cannot trigger MAC authentication.
- In the rules, only the action keyword (permit or deny) and the source IP match criterion can take effect.
- As a best practice, configure a deny rule to exclude the IPv6 IP addresses that start with fe80 from triggering MAC authentication.
- If you configure permit rules, add a **deny all** rule at the bottom of the ACL.

Do not use this command in conjunction with the **mac-authentication guest-vlan** command on a port. If both commands are used, the device cannot perform MAC authentication for a user once that user is added to the MAC authentication guest VLAN.

Examples

Include user IP addresses in MAC authentication requests on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication carry user-ip
```

Include user IP addresses in MAC authentication requests on GigabitEthernet 1/0/1 and deny users that use IPv6 link-local addresses from performing MAC authentication on the port.

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2000
[Sysname-acl-ipv6-basic-2000] rule deny source fe80:0::0:0 16
[Sysname-acl-ipv6-basic-2000] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication carry user-ip exclude-ip acl 2000
```

Related commands

mac-authentication

mac-authentication critical vlan

Use **mac-authentication critical vlan** to configure a MAC authentication critical VLAN on a port.

Use **undo mac-authentication critical vlan** to restore the default.

Syntax

mac-authentication critical vlan *critical-vlan-id*

undo mac-authentication critical vlan

Default

No MAC authentication critical VLAN exists on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

critical-vlan-id: Specifies a VLAN as the MAC authentication critical VLAN. The value range for the VLAN ID is 1 to 4094. Make sure the VLAN has been created.

Usage guidelines

The MAC authentication critical VLAN accommodates users that have failed MAC authentication because all the servers in their ISP domains are unreachable. Users in the critical VLAN can access network resources in the critical VLAN.

The critical VLAN feature takes effect when MAC authentication is performed only through RADIUS servers. If a MAC authentication user fails local authentication after RADIUS authentication, the user is not assigned to the critical VLAN.

Before you delete a VLAN that has been set as a MAC authentication critical VLAN, use the **undo mac-authentication critical vlan** command to remove the critical VLAN configuration.

Examples

Configure VLAN 100 as the MAC authentication critical VLAN on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication critical vlan 100
```

Related commands

display mac-authentication

reset mac-authentication critical vlan

mac-authentication critical-voice-vlan

Use **mac-authentication critical-voice-vlan** to enable the MAC authentication critical voice VLAN feature on a port.

Use **undo mac-authentication critical-voice-vlan** to restore the default.

NOTE:

This command is not supported on the following switch series:

- S5000E-X.
- S5110V2-SI.
- S5000V3-EI.
- S5000V5-EI.
- S5000X-EI.
- WAS6000.

Syntax

mac-authentication critical-voice-vlan

undo mac-authentication critical-voice-vlan

Default

The MAC authentication critical voice VLAN feature is disabled on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

The MAC authentication critical voice VLAN on a port accommodates MAC authentication voice users that have failed authentication because none of the RADIUS servers in their ISP domain are reachable.

Before you enable the MAC authentication critical voice VLAN feature on the port, make sure the following requirements are met:

- The port is configured with the voice VLAN.

  To configure a voice VLAN on a port, use the **voice-vlan enable** command (see *Layer 2—LAN Switching Command Reference*).

- LLDP is enabled both globally and on the port.

  The device uses LLDP to identify voice users. For information about LLDP commands, see *Layer 2—LAN Switching Command Reference*.
- A MAC authentication critical VLAN is configured on the port. This setting ensures that a voice user is assigned to the critical VLAN if it has failed authentication for unreachability of RADIUS servers before the device recognizes it as a voice user. If a MAC authentication critical VLAN is not available, the voice user might be logged off instead.

Examples

Enable the MAC authentication critical voice VLAN feature on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication critical-voice-vlan
```

Related commands

display mac-authentication

lldp enable (*Layer 2—LAN Switching Command Reference*)

lldp global enable (*Layer 2—LAN Switching Command Reference*)

reset mac-authentication critical-voice-vlan

voice-vlan enable (*Layer 2—LAN Switching Command Reference*)

mac-authentication domain

Use **mac-authentication domain** to specify a global or port-specific authentication domain.

Use **undo mac-authentication domain** to restore the default.

Syntax

mac-authentication domain *domain-name*

undo mac-authentication domain

Default

The system default authentication domain is used. For more information about the default authentication domain, see the **domain default enable** command in "AAA commands."

Views

System view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

domain-name: Specifies the name of an ISP domain, a case-insensitive string of 1 to 255 characters.

Usage guidelines

The global authentication domain applies to all MAC authentication-enabled ports. An authentication domain specified in Layer 2 Ethernet interface view applies only to the port. You can specify different authentication domains on different ports.

A port chooses an authentication domain for MAC authentication users in the following order:

1. Authentication domain specified on the port.

2. Global authentication domain specified in system view.
3. Default authentication domain.

Examples

Specify ISP domain **domain1** as the global MAC authentication domain.

```
<Sysname> system-view
[Sysname] mac-authentication domain domain1
```

Specify ISP domain **aabbcc** as the MAC authentication domain on GigabitEthernet 1/0/1.

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication domain aabbcc
```

Related commands

display mac-authentication

domain default enable

mac-authentication guest-vlan

Use **mac-authentication guest-vlan** to configure a MAC authentication guest VLAN on a port.

Use **undo mac-authentication guest-vlan** to restore the default.

Syntax

mac-authentication guest-vlan *guest-vlan-id*

undo mac-authentication guest-vlan

Default

No MAC authentication guest VLAN exists on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

guest-vlan-id: Specifies a VLAN as the MAC authentication guest VLAN. The value range for the VLAN ID is 1 to 4094. Make sure the VLAN has been created.

Usage guidelines

The MAC authentication guest VLAN accommodates users that have failed MAC authentication for any reason other than server unreachable. For example, the VLAN accommodates users with invalid passwords entered. You can deploy a limited set of network resources in the MAC authentication guest VLAN. For example, a software server for downloading software and system patches.

Before you delete a VLAN that has been set as a MAC authentication guest VLAN, use the **undo mac-authentication guest-vlan** command to remove the guest VLAN configuration.

Examples

Configure VLAN 100 as the MAC authentication guest VLAN on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication guest-vlan 100
```

Related commands

display mac-authentication

reset mac-authentication guest-vlan

mac-authentication guest-vlan auth-period

Use **mac-authentication guest-vlan auth-period** to set the interval at which the device authenticates users in the MAC authentication guest VLAN.

Use **undo mac-authentication guest-vlan auth-period** to restore the default.

Syntax

mac-authentication guest-vlan auth-period *period-value*

undo mac-authentication guest-vlan auth-period

Default

The device authenticates users in the MAC authentication guest VLAN every 30 seconds.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

period-value: Sets the authentication interval for users in the MAC authentication guest VLAN. The value range is 1 to 3600, in seconds.

Examples

Set the authentication interval to 150 seconds for users in the MAC authentication guest VLAN on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication guest-vlan auth-period 150
```

Related commands

display mac-authentication

mac-authentication guest-vlan

mac-authentication host-mode multi-vlan

Use **mac-authentication host-mode multi-vlan** to enable multi-VLAN mode for MAC authentication users on a port.

Use **undo mac-authentication host-mode** to restore the default.

Syntax

mac-authentication host-mode multi-vlan

undo mac-authentication host-mode

Default

MAC authentication operates in single-VLAN mode on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

To accommodate IP phone services or any other applications that are sensitive to delay or service interruption in a multi-VLAN environment, enable MAC authentication multi-VLAN mode.

In multi-VLAN mode, the port forwards traffic from a user in different VLANs without reauthentication if the user has been authenticated and come online in any VLAN on the port. Free of reauthentication, traffic from an online user can be sent in different VLANs without delay or service interruption.

Examples

Enable MAC authentication multi-VLAN mode on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication host-mode multi-vlan
```

Related commands

display mac-authentication

port-security mac-move permit

mac-authentication mac-range-account

Use **mac-authentication mac-range-account** to configure a username and password for MAC authentication users in a MAC address range.

Use **undo mac-authentication mac-range-account** to restore the default.

Syntax

mac-authentication mac-range-account mac-address *mac-address* **mask** { *mask* | *mask-length* } **account** *name* **password** { **cipher** | **simple** } *string*

undo mac-authentication mac-range-account { **all** | **mac-address** *mac-address* }

Default

No username or password is specifically configured for MAC authentication users in a MAC address range. The global user account policy applies to the users.

Views

System view

Predefined user roles

network-admin

Parameters

mac-address *mac-address*: Specifies a MAC address in the format of H-H-H.

mask *mask*: Specifies a MAC address mask, in the format of H-H-H. Make sure the most significant bits of the MAC address mask in binary format are consecutive 1s.

mask *mask-length*: Specifies a MAC address mask length, in the range of 1 to 48.

account *name*: Specifies a username. The name is a case-sensitive string of 1 to 55 characters, and cannot include the at sign (@).

password: Specifies the user password.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 63 characters. Its encrypted form is a case-sensitive string of 1 to 117 characters.

all: Specifies all MAC address ranges.

Usage guidelines

This command is supported only in Release 6310 or later.

Use this command to configure user account settings for users in a MAC address range (for example, users with a specific OUI). For users in the specified range, this command has higher priority than the **mac-authentication user-name-format** command.

You can configure a maximum of 16 MAC address ranges. However, you must make sure the MAC address ranges do not overlap.

If you configure user account settings multiple times for the same MAC address range, the most recent configuration overwrites the previous configuration.

The **mac-authentication mac-range-account** command applies only to unicast MAC addresses.

- If you specify a MAC address range that contains only multicast MAC addresses, execution of this command will fail.
- If you specify a MAC address range that contains both unicast and multicast MAC addresses, the command takes effect only on unicast MAC addresses.

The all-zero MAC address is invalid for MAC authentication. Users with the all-zero MAC address cannot pass MAC authentication.

Examples

Configure a user account for MAC addresses that start with **aaaa**. Set the MAC address mask to **ffff-0000-0000**, the username to **user1**, and the password to **1234** in plaintext form.

```
<Sysname> system-view
[Sysname] mac-authentication mac-range-account mac-address aaaa-0000-0000 mask
ffff-0000-0000 account user1 password simple 1234
```

Related commands

display mac-authentication

mac-authentication user-name-format

mac-authentication max-user

Use **mac-authentication max-user** to set the maximum number of concurrent MAC authentication users on a port.

Use **undo mac-authentication max-user** to restore the default.

Syntax

mac-authentication max-user *max-number*

undo mac-authentication max-user

Default

A port allows a maximum of 4294967295 concurrent MAC authentication users.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

max-number: Sets the maximum number of concurrent MAC authentication users on the port. The value range for this argument is 1 to 4294967295.

Usage guidelines

Set the maximum number of concurrent MAC authentication users on a port to prevent the system resources from being overused. When the maximum number is reached, the port denies subsequent MAC authentication users.

Examples

Configure GigabitEthernet 1/0/1 to support a maximum of 32 concurrent MAC authentication users.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication max-user 32
```

Related commands

display mac-authentication

mac-authentication offline-detect enable

Use **mac-authentication offline-detect enable** to enable MAC authentication offline detection on a port.

Use **undo mac-authentication offline-detect enable** to disable MAC authentication offline detection.

Syntax

mac-authentication offline-detect enable

undo mac-authentication offline-detect enable

Default

MAC authentication offline detection is enabled on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

IMPORTANT:

When MAC authentication offline detection is used, make sure the aging timer value for dynamic MAC address entries is less than or equal to the default offline detection timer value (300 seconds) for MAC authentication users. The aging timer for dynamic MAC address entries is configurable with the **mac-address timer aging** *seconds* command.

The MAC authentication offline detection feature monitors the online status of MAC authentication users. This feature uses an offline detection timer to set the interval that the device must wait for traffic from a user before the device determines that the user is idle. If the device has not received traffic from a user before the timer expires, the device logs off that user and requests the accounting server to stop accounting for the user.

To set the offline detection timer, use the **mac-authentication timer** command.

Examples

Disable MAC authentication offline detection on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo mac-authentication offline-detect enable
```

Related commands

mac-authentication timer

mac-authentication offline-detect mac-address

Use **mac-authentication offline-detect mac-address** to configure MAC authentication offline detection for a MAC authentication user.

Use **undo mac-authentication offline-detect mac-address** to restore the default.

Syntax

mac-authentication offline-detect mac-address *mac-address* { **ignore** | **timer** *offline-detect-value* [**check-arp-or-nd-snooping**] }

undo mac-authentication offline-detect mac-address *mac-address*

Default

The offline detection settings configured on access ports take effect and the offline detection timer set in system view is used.

Views

System view

Predefined user roles

network-admin

Parameters

mac-address: Specifies a MAC address in the format of H-H-H, excluding multicast, all-zero, and all-F MAC addresses.

ignore: Skips offline detection for the specified user.

timer *offline-detect-value*: Specifies the offline detection timer for the specified user. The value range is 60 to 2147483647 seconds.

check-arp-or-nd-snooping: Uses the ARP snooping or ND snooping table in offline detection to determine the offline state of the user.

Usage guidelines

Use this command to set offline detection parameters specific to a MAC authentication user. To have this command take effect, you must make sure MAC authentication offline detection is enabled on the user's access port. The user-specific offline detection settings take effect on the online users immediately after they are configured.

Use this command as follows:

- Set an offline detection timer specific to a user and control whether to use the ARP snooping or ND snooping table to determine the offline state of the user.
  - If the ARP snooping or ND snooping table is used, the device searches the ARP snooping or ND snooping table before it checks for traffic from the user within the detection interval. If a matching ARP snooping or ND snooping entry is found, the device resets the offline detection timer and the user stays online. If the offline detection timer expires because the device has not found a matching snooping entry for the user or received traffic from the user, the device disconnects the user.
  - If the ARP or ND snooping table is not used, the device disconnects the user if it has not received traffic from that user before the offline detection timer expires.

  When disconnecting the user, the device also notifies the RADIUS server (if any) to stop user accounting.
- Skip offline detection for the user. You can choose this option if the user is a dumb terminal. A dumb terminal might fail to come online again after it is logged off by the offline detection feature.

The device uses the offline detection settings for a user in the following sequence:

1. User-specific offline detection settings.
2. Offline detection settings assigned to the user by the RADIUS server. The settings include the offline detection timer, use of the ARP or ND snooping table in offline detection, and whether to ignore offline detection.
3. Port-based offline detection settings.

Examples

Disable MAC authentication offline detection for the MAC authentication user with MAC address 000a-eb29-7511.

```
<Sysname> system-view
[Sysname] mac-authentication offline-detect mac-address 000a-eb29-7511 ignore
```

Enable MAC authentication offline detection for the MAC authentication user with MAC address 000a-eb29-7511, and set the offline detection timer to 24 hours.

```
<Sysname> system-view
[Sysname] mac-authentication offline-detect mac-address 000a-eb29-7511 timer 86400
```

Related commands

display mac-authentication connection

mac-authentication offline-detect enable

mac-authentication timer (system view)

mac-authentication packet-detect enable

Use **mac-authentication packet-detect enable** to enable packet detection for MAC authentication.

Use **undo mac-authentication packet-detect enable** to restore the default.

Syntax

mac-authentication packet-detect enable

undo mac-authentication packet-detect enable

Default

Packet detection for MAC authentication is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

This command is supported only in Release 6348P01 and later.

When packet detection for MAC authentication is enabled on a port, the device sends detection packets to MAC authentication users connected to that port at offline detection intervals set by using the offline detection timer. If the device does not receive a response from a user after it has made the maximum packet transmission attempts within an offline detection interval, it logs off that user and requests the RADIUS server to stop accounting for the user.

When packet detection for MAC authentication and MAC authentication offline detection are both enabled, the device processes a MAC authentication user as follows:

- If MAC authentication offline detection determines that a user is online, the device does not send detection packets to that user.
- If MAC authentication offline detection determines that a user is offline, the device does not immediately logs off that user. Instead, the device sends a detection packet to that user. It will log off that user if it does not receive a response from that user after it has made the maximum packet transmission attempts within an offline detection interval.

MAC authentication uses ARP request packets to detect the online status of IPv4 users and uses NS packets to detect the online status of IPv6 users.

To ensure that the device is aware of user IP address changes, enable ARP snooping and ND snooping in conjunction with packet detection for MAC authentication. If you do not enable ARP snooping or ND snooping, the device is unaware of user IP address changes. As a result, the device still sends detection packets to the users' original IP addresses and falsely log off these users.

Examples

Enable packet detection for MAC authentication on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication packet-detect enable
```

Related commands

mac-authentication timer offline-detect

port-security packet-detect arp-source-ip factor

mac-authentication packet-detect retry

mac-authentication packet-detect retry

Use **mac-authentication packet-detect retry** to set the maximum number of attempts for sending a detection packet to a MAC authentication user.

Use **undo mac-authentication packet-detect retry** to restore the default.

Syntax

mac-authentication packet-detect retry *retries*

undo mac-authentication packet-detect retry

Default

The device sends a detection packet to a MAC authentication user for a maximum of two times.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

retries: Sets the maximum number of attempts for sending a detection packet to a MAC authentication user. The value range is 1 to 10.

Usage guidelines

This command is supported only in Release 6348P01 and later.

When packet detection for MAC authentication is enabled on a port, the device sends detection packets to MAC authentication users connected to that port at offline detection intervals set by using the offline detection timer. If the device does not receive a response from a user after it has made the maximum packet transmission attempts within an offline detection interval, it logs off that user and requests the RADIUS server to stop accounting for the user.

To prevent a MAC authentication user from being logged off because the device does not obtain the IP address of that user when that user just comes online, the device increases the maximum number of packet transmission attempts by 10 on the basis of the original configuration.

Examples

On GigabitEthernet 1/0/1, set the maximum number of attempts to 8 for sending a detection packet to a MAC authentication user.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication packet-detect retry 8
```

Related commands

mac-authentication packet-detect enable

mac-authentication parallel-with-dot1x

Use **mac-authentication parallel-with-dot1x** to enable parallel processing of MAC authentication and 802.1X authentication on a port.

Use **undo mac-authentication parallel-with-dot1x** to restore the default.

Syntax

mac-authentication parallel-with-dot1x

undo mac-authentication parallel-with-dot1x

Default

Parallel processing of MAC authentication and 802.1X authentication is disabled on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

When you configure this command on a port, follow these restrictions and guidelines:

- Make sure the port meets the following requirements:

    - The port is configured with both 802.1X authentication and MAC authentication and performs MAC-based access control for 802.1X authentication.
    - The port is enabled with the 802.1X unicast trigger.
- For the port to perform MAC authentication before it is assigned to the 802.1X guest VLAN, use the **dot1x guest-vlan-delay new-mac** command to delay assigning the port to the 802.1X guest VLAN.

  For information about the **dot1x guest-vlan-delay new-mac** command, see "802.1X commands."
- Do not enable MAC authentication delay on the port. This operation will delay MAC authentication after 802.1X authentication is triggered.
- To configure both 802.1X authentication and MAC authentication on the port, use one of the following methods:
    - Enable the 802.1X and MAC authentication features separately on the port.
    - Enable port security on the port. The port security mode must be **userlogin-secure-or-mac** or **userlogin-secure-or-mac-ext**.

      For information about port security mode configuration, see port security in *Security Configuration Guide*.

Examples

Enable parallel processing of MAC authentication and 802.1X authentication on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication parallel-with-dot1x
```

Related commands

display mac-authentication

mac-authentication re-authenticate

Use **mac-authentication re-authenticate** to enable the periodic MAC reauthentication feature on a port.

Use **undo mac-authentication re-authenticate** to disable the periodic MAC reauthentication feature on a port.

Syntax

mac-authentication re-authenticate

undo mac-authentication re-authenticate

Default

The periodic MAC reauthentication feature is disabled on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

Periodic MAC reauthentication enables the access device to periodically authenticate online MAC authentication users on a port. This feature tracks the connection status of online users and updates the authorization attributes assigned by the server, such as the ACL and VLAN.

To set the periodic reauthentication timer, use the **mac-authentication timer reauth-period** command in system view or in Ethernet interface view.

If periodic reauthentication is triggered for a user while that user is waiting for online synchronization, the system performs online synchronization and does not perform reauthentication for the user.

Examples

Enable the periodic MAC reauthentication feature on GigabitEthernet 1/0/1 and set the global periodic reauthentication timer to 1800 seconds.

```
<Sysname> system-view
[Sysname] mac-authentication timer reauth-period 1800
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication re-authenticate
```

Related commands

display mac-authentication

mac-authentication server-recovery online-user-sync

mac-authentication timer

mac-authentication re-authenticate server-unreachable keep-online

Use **mac-authentication re-authenticate server-unreachable keep-online** to enable the keep-online feature on a port.

Use **undo mac-authentication re-authenticate server-unreachable** to restore the default.

Syntax

mac-authentication re-authenticate server-unreachable keep-online

undo mac-authentication re-authenticate server-unreachable

Default

The keep-online feature is disabled on a port. The device logs off online MAC authentication users if no server is reachable for MAC reauthentication.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

The keep-online feature keeps authenticated MAC authentication users online when no server is reachable for MAC reauthentication.

Examples

Enable the keep-online feature for authenticated MAC authentication users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication re-authenticate server-unreachable
keep-online
```

Related commands

display mac-authentication

mac-authentication server-recovery online-user-sync

Use **mac-authentication server-recovery online-user-sync** to enable online user synchronization for MAC authentication.

Use **undo mac-authentication server-recovery online-user-sync** to disable online user synchronization for MAC authentication.

Syntax

mac-authentication server-recovery online-user-sync

undo mac-authentication server-recovery online-user-sync

Default

Online user synchronization for MAC authentication is disabled. The device does not synchronize online MAC authentication user information on a port with a RADIUS server after the RADIUS server recovers from the unreachable state.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

IMPORTANT:

This command takes effect only when the device uses an IMC RADIUS server to authenticate MAC authentication users.

To ensure that the RADIUS server maintains the same online MAC authentication user information as the device after the server state changes from unreachable to reachable, use this feature.

This feature synchronizes online MAC authentication user information between the device and the RADIUS server when the RADIUS server state is detected having changed from unreachable to reachable.

When synchronizing online MAC authentication user information on a port with the RADIUS server, the device initiates MAC authentication in turn for each authenticated online MAC authentication user to the RADIUS server.

If synchronization fails for an online user, the device logs off that user unless the failure occurs because the server has become unreachable again.

The amount of time required to complete online user synchronization increases as the number of online users grows. This might result in an increased delay for new MAC authentication users and users in the critical VLAN to authenticate or reauthenticate to the RADIUS server and come online.

To have this feature take effect, you must use it in conjunction with the RADIUS server status detection feature, which is configurable with the **radius-server test-profile** command. For more information about the RADIUS server status detection feature, see AAA configuration in *Security Configuration Guide*.

Examples

Enable online user synchronization for MAC authentication on GigabitEthernet 1/0/1.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication server-recovery online-user-sync
```

Related commands

display mac-authentication

radius-server test-profile

timer quiet (RADIUS scheme view)

mac-authentication timer (interface view)

Use **mac-authentication timer** to configure a MAC authentication timer on a port.

Use **undo mac-authentication timer** to restore the default of a MAC authentication timer.

Syntax

mac-authentication timer { **auth-delay** *auth-delay-time* | **reauth-period** *reauth-period-value* }

undo mac-authentication timer { **auth-delay** | **reauth-period** }

Default

No MAC authentication delay timer is set on a port. MAC authentication delay is disabled. MAC authentication starts immediately after it is triggered by a user packet.

No periodic MAC reauthentication timer is set on a port. The port uses the global periodic MAC reauthentication timer.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

auth-delay *auth-delay-time*: Sets the delay time for MAC authentication in seconds. The value range is 1 to 180.

reauth-period *reauth-period-value*: Sets the port-specific periodic MAC reauthentication timer in seconds. The value range is 60 to 7200 prior to Release 6343P08. As from Release 6343P08, the value range for this timer is 60 to 86400.

Usage guidelines

When both 802.1X authentication and MAC authentication are enabled on a port, you can delay MAC authentication so that 802.1X authentication is preferentially triggered. If no 802.1X authentication is triggered or if 802.1X authentication fails within the delay period, the port continues to process MAC authentication.

Do not set the port security mode to **mac-else-userlogin-secure** or **mac-else-userlogin-secure-ext** when you want to use MAC authentication delay. The delay does not take effect on a port in either of the two modes. For more information about port security modes, see "Port security commands."

The device reauthenticates online MAC authentication users on a port at the specified periodic reauthentication interval if the port is enabled with periodic MAC reauthentication. To enable periodic MAC reauthentication on a port, use the **mac-authentication re-authenticate** command.

A change to the port-specific periodic reauthentication timer applies to online users only after the old timer expires.

The device selects a periodic reauthentication timer for MAC reauthentication in the following order:

1. Server-assigned reauthentication timer.
2. Port-specific reauthentication timer.
3. Global reauthentication timer.
4. Default reauthentication timer.

Examples

Enable MAC authentication delay on GigabitEthernet 1/0/1 and set the delay time to 10 seconds.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication timer auth-delay 10
```

Related commands

display mac-authentication

port-security port-mode

mac-authentication timer (system view)

Use **mac-authentication timer** to configure a MAC authentication timer.

Use **undo mac-authentication timer** to restore the default of a MAC authentication timer.

Syntax

mac-authentication timer { **offline-detect** *offline-detect-value* | **quiet** *quiet-value* | **reauth-period** *reauth-period-value* | **server-timeout** *server-timeout-value* | **user-aging** { **critical-vlan** | **guest-vlan** } *aging-time-value* }

undo mac-authentication timer { **offline-detect** | **quiet** | **reauth-period** | **server-timeout** | **user-aging** { **critical-vlan** | **guest-vlan** } }

Default

The following MAC authentication timers apply:

- The offline detection timer is 300 seconds.
- The quiet timer is 60 seconds.
- The global periodic MAC reauthentication timer is 3600 seconds.
- The server timeout timer is 100 seconds.
- User aging timer for a type of MAC authentication VLAN: 1000 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

offline-detect *offline-detect-value*: Sets the offline detection timer. The value range is 60 to 2147483647 seconds.

quiet *quiet-value*: Sets the quiet timer. The value range is 1 to 3600 seconds.

reauth-period *reauth-period-value*: Sets the global periodic MAC reauthentication timer, in seconds. The value range is 60 to 7200 prior to Release 6343P08. As from Release 6343P08, the value range for this timer is 60 to 86400.

server-timeout *server-timeout-value*: Sets the server timeout timer. The value range is 100 to 300 seconds.

user-aging: Sets the user aging timer for a type of MAC authentication VLAN.

critical-vlan: Specifies MAC authentication critical VLANs.

guest-vlan: Specifies MAC authentication guest VLANs.

aging-time-value: Sets the user aging timer. The value range is 60 to 2147483647 seconds.

Usage guidelines

MAC authentication uses the following timers:

- **Offline detection timer**—Sets the interval that the device must wait for traffic from a user before the device determines that the user is idle. If the device has not received traffic from a user before the timer expires, the device logs off that user and requests the accounting server to stop accounting for the user. This timer takes effect only when the MAC authentication offline detection feature is enabled.

  As a best practice, set the MAC address aging timer to the same value as the offline detection timer. This operation prevents a MAC authenticated user from being logged off within the offline detect interval because of MAC address entry expiration.
- **Quiet timer**—Sets the interval that the device must wait before the device can perform MAC authentication for a user that has failed MAC authentication. All packets from the MAC address are dropped during the quiet time. This quiet mechanism prevents repeated authentication from affecting system performance.
- **Periodic MAC reauthentication timer**—Sets the interval at which the device reauthenticates online MAC authentication users on a port if the port is enabled with periodic MAC reauthentication. A change to the global periodic reauthentication timer applies to online users only after the old timer expires.
- **Server timeout timer**—Sets the interval that the device waits for a response from a RADIUS server before the device determines that the RADIUS server is unavailable. If the timer expires during MAC authentication, the user fails MAC authentication.

  To avoid forced logoff before the server timeout timer expires, set the server timeout timer to a value that is lower than or equal to the product of the following values:

  - The maximum number of RADIUS packet transmission attempts set by using the **retry** command in RADIUS scheme view.
  - The RADIUS server response timeout timer set by using the **timer response-timeout** command in RADIUS scheme view.

  For information about setting the maximum number of RADIUS packet transmission attempts and the RADIUS server response timeout timer, see AAA configuration in *Security Configuration Guide*.
- **User aging timer (user-aging)**—Sets the user aging timer for a type of MAC authentication VLAN.

  If you enable user aging for unthenticated MAC authentication user, you can set a user aging timer for MAC authentication critical or guest VLANs. The user aging timer for a type of MAC authentication VLAN determines how long a user can stay in that type of VLAN.

  For more information about how user aging operates, see the usage guidelines for the **mac-authentication unauthenticated-user aging enable** command.

  Do not set the user aging timer for users in MAC authentication guest VLANs to a multiple of the authentication interval for them. If you do so, the aging timer will not take effect. The authentication interval for MAC authentication users in a guest VLAN is configurable with the **mac-authentication guest-vlan auth-period** command.

Examples

Set the server timeout timer to 150 seconds.

```
<Sysname> system-view
[Sysname] mac-authentication timer server-timeout 150
```

Related commands

display mac-authentication

mac-authentication guest-vlan auth-period

mac-authentication unauthenticated-user aging enable

retry

timer response-timeout (RADIUS scheme view)

mac-authentication unauthenticated-user aging enable

Use **mac-authentication unauthenticated-user aging enable** to enable unauthenticated MAC authentication user aging.

Use **undo mac-authentication unauthenticated-user aging enable** to disable unauthenticated MAC authentication user aging.

Syntax

mac-authentication unauthenticated-user aging enable

undo mac-authentication unauthenticated-user aging enable

Default

Unauthenticated MAC authentication user aging is enabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

Unauthenticated MAC authentication user aging applies to users added to a MAC authentication guest or critical VLAN because they have not been authenticated or have failed authentication.

When a user in one of those VLANs ages out, the device removes the user from the VLAN and deletes the MAC address entry for the user from the access port.

For users in one of those VLANs on one port to be authenticated successfully and come online on another port, enable this feature. In any other scenarios, disable this feature as a best practice.

Examples

Disable unauthenticated MAC authentication user aging on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo mac-authentication unauthenticated-user aging enable
```

Related commands

mac-authentication timer

mac-authentication user-name-format

Use **mac-authentication user-name-format** to configure the type of user accounts for MAC authentication users.

Use **undo mac-authentication user-name-format** to restore the default.

Syntax

mac-authentication user-name-format { **fixed** [**account** *name*] | **mac-address** [{ **with-hyphen** [**separator colon**] | **without-hyphen** } [**lowercase** | **uppercase**]] } [**password** { **cipher** | **simple** } *string*]

undo mac-authentication user-name-format

Default

Each user's MAC address is used as the username and password for MAC authentication. A MAC address is in hexadecimal notation without hyphens, and letters are in lower case.

Views

System view

Predefined user roles

network-admin

Parameters

fixed: Uses a shared account for all MAC authentication users.

account *name*: Specifies the username for the shared account. The name is a case-sensitive string of 1 to 55 characters, excluding the at sign (@). If you do not specify a username, the default name **mac** applies.

mac-address: Uses MAC-based user accounts for MAC authentication users.

with-hyphen: Includes hyphens in MAC addresses. The MAC addresses use the xx-xx-xx-xx-xx-xx format or the XX-XX-XX-XX-XX-XX format.

separator colon: Uses the colon (:) in place of the hyhen (-) as the separator in MAC addresses. The MAC addresses use the xx:xx:xx:xx:xx:xx format or the XX:XX:XX:XX:XX:XX format. If you do not specify the colon as the separator, the hypen is used. The colon seperator is supported only in Release 6340 and later.

without-hyphen: Excludes hyphens from a MAC address, for example, xxxxxxxxxxxx.

lowercase: Specifies letters in lower case.

uppercase: Specifies letters in upper case.

password: Specifies the user password. If you do not specify a password for MAC-based user accounts, the device uses the MAC address of each user in the specified format as the password. If you do not specify a password for the shared account, the shared account does not have a password.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 63 characters. Its encrypted form is a case-sensitive string of 1 to 117 characters.

Usage guidelines

If you specify the MAC-based user account format, the device uses the MAC address of a user as the username for MAC authentication of the user. This user account type ensures high authentication security. However, you must create on the authentication server a user account for each user, using the MAC address of the user as the username.

If you specify a shared user account, the device uses the specified username and password for MAC authentication of all users. Because all MAC authentication users use a single account for

authentication, you only need to create one account on the authentication server. This user account type is suitable for trusted networks.

Examples

Configure a shared account for MAC authentication users, and set the username to **abc** and password to plaintext string of **xyz**.

```
<Sysname> system-view
[Sysname] mac-authentication user-name-format fixed account abc password simple xyz
```

Use the MAC address of each user as both the username and password for MAC authentication. The MAC addresses are in hexadecimal notation with hyphens, and letters are in upper case.

```
<Sysname> system-view
[Sysname] mac-authentication user-name-format mac-address with-hyphen uppercase
```

Related commands

display mac-authentication

reset mac-authentication access-user

Use **reset mac-authentication access-user** to log off MAC authentication users.

Syntax

reset mac-authentication access-user [**interface** *interface-type interface-number* | **mac** *mac-address* | **username** *username* | **vlan** *vlan-id*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

mac *mac-address*: Specifies a MAC authentication user by its MAC address. The *mac-address* argument is in the format of H-H-H.

username *username*: Specifies a MAC authentication user by its name. The *username* argument is a case-sensitive string of 1 to 253 characters.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

This command is supported only in Release 6318P01 and later.

Use this command to log off the specified MAC authentication users and clear information about these users from the device. These users must perform MAC authentication to come online again.

With a VLAN specified, this command logs off the following MAC authentication users:

- Users that have passed MAC authentication and have been assigned the specified VLAN as their authorization VLAN by the server.
- Users that stay in the specified VLAN after they have passed MAC authentication, because they have not been assigned an authorization VLAN yet.
- Users that are performing MAC authentication in the specified VLAN.

To identify the VLAN in which a user is staying, use the **display mac-address** command.

If you do not specify any parameters, the **reset mac-authentication access-user** command logs off all MAC authentication users on the device.

Examples

Log off all MAC authentication users on GigabitEthernet 1/0/1.

```
<Sysname> reset mac-authentication access-user interface gigabitethernet 1/0/1
```

Related commands

display mac-authentication connection

reset mac-authentication critical vlan

Use **reset mac-authentication critical vlan** to remove users from the MAC authentication critical VLAN on a port.

Syntax

reset mac-authentication critical vlan interface *interface-type interface-number* [**mac-address** *mac-address*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

mac-address *mac-address*: Specifies a user by its MAC address. If you do not specify this option, the command removes all users from the MAC authentication critical VLAN on the port.

Examples

Remove the user with MAC address **1-1-1** from the MAC authentication critical VLAN on GigabitEthernet 1/0/1.

```
<Sysname> reset mac-authentication critical vlan interface gigabitethernet 1/0/1
mac-address 1-1-1
```

Related commands

display mac-authentication

mac-authentication critical vlan

reset mac-authentication critical-voice-vlan

Use **reset mac-authentication critical-voice-vlan** to remove MAC authentication users from the MAC authentication critical voice VLAN on a port.

Syntax

reset mac-authentication critical-voice-vlan interface *interface-type interface-number* [**mac-address** *mac-address*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

mac-address *mac-address*: Specifies a user by its MAC address. If you do not specify this option, the command removes all users from the MAC authentication critical voice VLAN on the port.

Examples

Remove the user with MAC address **1-1-1** from the MAC authentication critical voice VLAN on GigabitEthernet 1/0/1.

```
<Sysname> reset mac-authentication critical-voice-vlan interface gigabitethernet 1/0/1
mac-address 1-1-1
```

Related commands

display mac-authentication

mac-authentication critical-voice-vlan

reset mac-authentication guest-vlan

Use **reset mac-authentication guest-vlan** to remove users from the MAC authentication guest VLAN on a port.

Syntax

reset mac-authentication guest-vlan interface *interface-type interface-number* [**mac-address** *mac-address*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

mac-address *mac-address*: Specifies a user by its MAC address. If you do not specify this option, the command removes all users from the MAC authentication guest VLAN on the port.

Examples

Remove the user with MAC address **1-1-1** from the MAC authentication guest VLAN on GigabitEthernet 1/0/1.

```
<Sysname> reset mac-authentication guest-vlan interface gigabitethernet 1/0/1 mac-address
1-1-1
```

Related commands

display mac-authentication

mac-authentication guest-vlan

reset mac-authentication statistics

Use **reset mac-authentication statistics** to clear MAC authentication statistics.

Syntax

reset mac-authentication statistics [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify a port, this command clears both global and port-specific MAC authentication statistics.

Examples

Clear MAC authentication statistics on GigabitEthernet 1/0/1.

```
<Sysname> reset mac-authentication statistics interface gigabitethernet 1/0/1
```

Related commands

display mac-authentication

Contents

Portal commands

captive-bypass enable

Use **captive-bypass enable** to enable the captive-bypass feature.

Use **undo captive-bypass enable** to disable the captive-bypass feature.

Syntax

captive-bypass enable

undo captive-bypass enable

Default

The captive-bypass feature is disabled. The device automatically pushes the portal authentication page to the iOS devices and some Android devices when they are connected to the network.

Views

Portal Web server view

Predefined user roles

network-admin

Usage guidelines

With this feature enabled, the device does not automatically push the portal authentication page to iOS devices and some Android devices when they are connected to the network. The device pushes the portal authentication page only when the user accesses the Internet by using a browser.

Examples

Enable the captive-bypass feature.

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] captive-bypass enable
```

Related commands

display portal web-server

default-logon-page

Use **default-logon-page** to specify the default authentication page file for the local portal Web service.

Use **undo default-logon-page** to restore the default.

Syntax

default-logon-page *file-name*

undo default-logon-page

Default

The default authentication page file is **default.zip**.

Views

Local portal Web service view

Predefined user roles

network-admin

Parameters

file-name: Specifies the default authentication page file by the file name (without the file storage directory). The file name is a case-sensitive string of 1 to 91 characters. Valid characters are letters, digits, dots (.) and underscores (_).

Usage guidelines

After you use the **default-logon-page** command to specify the file, the device decompresses the file to get the authentication pages. The device then sets them as the default authentication pages for local portal authentication.

As a best practice for the correct operation of the local portal Web service, use the default authentication page file in the root directory of the device storage medium. To use custom authentication pages, you must strictly follow the related restrictions and guidelines when customizing your own authentication pages. For more information about the restrictions and guidelines, see portal authentication configuration in *Security Configuration Guide*.

Examples

Specify file **pagefile1.zip** as the default authentication page file for local portal authentication.

```
<Sysname> system-view
[Sysname] portal local-web-server http
[Sysname-portal-local-websvr-http] default-logon-page pagefile1.zip
```

Related commands

portal local-web-server

display portal

Use **display portal** to display portal configuration and portal running state.

Syntax

display portal interface *interface-type interface-number*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

Examples

Display portal configuration and portal running state on VLAN-interface 2.

```
<Sysname> display portal interface vlan-interface 2
 Portal information of Vlan-interface2
     NAS-ID profile: aaa
     Authorization : Strict checking
     ACL           : Enabled
     User profile  : Disabled
```

```
IPv4:
    Portal status: Enabled
    Portal authentication method: Direct
    Portal web server: wbs
    Secondary portal Web server: wbsec
    Portal mac-trigger-server: Not configured
    Authentication domain: my-domain
    User-dhcp-only: Enabled
    Pre-auth IP pool: ab
    Max Portal users: Not configured
    Bas-ip: Not configured
    User detection : Type: ICMP  Interval: 300s  Attempts: 5   Idle time: 180s
    Action for server detection:
        Server type    Server name                        Action
        Web server     wbs                                fail-permit
        Portal server  pts                                fail-permit
    Layer3 source network:
        IP address              Mask
        1.1.1.1                 255.255.0.0

    Destination authentication subnet:
        IP address              Mask
        2.2.2.2                 255.255.255.0

IPv6:
    portal status: Disabled
    Portal authentication method: Disabled
    Portal web server: Not configured
    Secondary portal Web server: Not configured
    Portal mac-trigger-server: Not configured
    Authentication domain: Not configured
    User-dhcp-only: Disabled
    Pre-auth IP pool: Not configured
    Max Portal users: Not configured
    Bas-ipv6:Not configured
    User detection: Not configured
    Action for server detection:
        Server type    Server name                        Action
        --             --                                 --
    Layer3 source network:
        IP address                                        Prefix length

    Destination authentication subnet:
        IP address                                        Prefix length
```

Table 1 Command output

Field	Description
Portal information of interface	Portal configuration on the interface.

NAS-ID profile	NAS-ID profile on the interface.
Authorization	Authorization information type: ACL or user profile.
Strict checking	Whether strict checking is enabled on portal authorization information.
IPv4	IPv4 portal configuration.
IPv6	IPv6 portal configuration.
Portal status	Portal authentication status on the interface: • **Disabled**—Portal authentication is disabled. • **Enabled**—Portal authentication is enabled. • **Authorized**—The portal authentication server or portal Web server is unreachable. The interface allows users to have network access without authentication.
Portal authentication method	Authentication mode enabled on the interface: • **Direct**—Direct authentication. • **Redhcp**—Re-DHCP authentication. • **Layer3**—Cross-subnet authentication.
Portal Web server	Name of the portal Web server specified on the interface.
Secondary portal Web server	Name of the secondary portal Web server specified on the interface. This field also displays **active** if the secondary Web server is being used. This field is supported only in Release 6348P01 and later.
Portal mac-trigger-server	This field is not supported in the current software version. Name of the MAC binding server specified on the interface.
Authentication domain	Mandatory authentication domain on the interface.
User-dhcp-only	Status of the user-dhcp-only feature: • **Enabled**—Only users with IP addresses obtained through DHCP can perform portal authentication. • **Disabled**—Both users with IP addresses obtained through DHCP and users with static IP addresses can pass authentication to get online.
Pre-auth ip-pool	Name of the IP address pool specified for portal users before authentication.
Max Portal users	Maximum number of portal users allowed on an interface.
Bas-ip	BAS-IP attribute of the portal packets sent to the portal authentication server.
Bas-ipv6	BAS-IPv6 attribute of the portal packets sent to the portal authentication server.
User detection	Configuration for online detection of portal users on the interface, including detection method (ARP, ICMP, ND, or ICMPv6), detection interval, maximum number of detection attempts, and user idle time.
Action for server detection	Portal server detection configuration on the interface: • **Server type**—Type of the server. **Portal server** represents the portal authentication server, and **Web server** represents the portal Web server. • **Server name**—Name of the server. • **Action**—Action triggered by the result of server detection. This field displays **fail-permit** when the portal fail-permit feature is enabled.

Layer3 source network	Information of the portal authentication source subnet.
Destination authentication subnet	Information of the portal authentication destination subnet.
IP address	IP address of the portal authentication subnet.
Mask	Subnet mask of the portal authentication subnet.
Prefix length	Prefix length of the IPv6 portal authentication subnet address.

Related commands

portal domain

portal enable

portal free-all except destination

portal ipv6 free-all except destination

portal ipv6 layer3 source

portal layer3 source

portal web-server

display portal packet statistics

Use **display portal packet statistics** to display packet statistics for portal authentication servers.

Syntax

display portal packet statistics [**server** *server-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

server *server-name*: Specifies a portal authentication server by its name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

This command displays statistics on packets the device sent to and received from portal authentication servers.

If you do not specify the **server** *server-name* option, this command displays packet statistics for all portal authentication servers.

Examples

Display packet statistics for portal authentication server **pts**.

```
<Sysname> display portal packet statistics server pts
 Portal server :  pts
 Invalid packets: 0
 Pkt-Type                          Total    Drops    Errors
```

```
REQ_CHALLENGE                3         0         0
ACK_CHALLENGE                3         0         0
REQ_AUTH                     3         0         0
ACK_AUTH                     3         0         0
REQ_LOGOUT                   1         0         0
ACK_LOGOUT                   1         0         0
AFF_ACK_AUTH                 3         0         0
NTF_LOGOUT                   1         0         0
REQ_INFO                     6         0         0
ACK_INFO                     6         0         0
NTF_USERDISCOVER             0         0         0
NTF_USERIPCHANGE             0         0         0
AFF_NTF_USERIPCHAN           0         0         0
ACK_NTF_LOGOUT               1         0         0
NTF_HEARTBEAT                0         0         0
NTF_USER_HEARTBEAT           2         0         0
ACK_NTF_USER_HEARTBEAT       0         0         0
NTF_CHALLENGE                0         0         0
NTF_USER_NOTIFY              0         0         0
AFF_NTF_USER_NOTIFY          0         0         0
```

Table 2 Command output

Field	Description
Portal server	Name of the portal authentication server.
Invalid packets	Number of invalid packets.
Pkt-Type	Packet type.
Total	Total number of packets.
Drops	Number of dropped packets.
Errors	Number of packets that carry error information.
REQ_CHALLENGE	Challenge request packet the portal authentication server sent to the access device.
ACK_CHALLENGE	Challenge acknowledgment packet the access device sent to the portal authentication server.
REQ_AUTH	Authentication request packet the portal authentication server sent to the access device.
ACK_AUTH	Authentication acknowledgment packet the access device sent to the portal authentication server.
REQ_LOGOUT	Logout request packet the portal authentication server sent to the access device.
ACK_LOGOUT	Logout acknowledgment packet the access device sent to the portal authentication server.
AFF_ACK_AUTH	Affirmation packet the portal authentication server sent to the access device after receiving an authentication acknowledgment packet.
NTF_LOGOUT	Forced logout notification packet the access device sent to the portal authentication server.

REQ_INFO	Information request packet.
ACK_INFO	Information acknowledgment packet.
NTF_USERDISCOVER	User discovery notification packet the portal authentication server sent to the access device.
NTF_USERIPCHANGE	User IP change notification packet the access device sent to the portal authentication server.
AFF_NTF_USERIPCHAN	User IP change success notification packet the portal authentication server sent to the access device.
ACK_NTF_LOGOUT	Forced logout acknowledgment packet the portal authentication server sent to the access device.
NTF_HEARTBEAT	Server heartbeat packet the portal authentication server periodically sent to the access device.
NTF_USER_HEARTBEAT	User synchronization packet the portal authentication server sent to the access device.
ACK_NTF_USER_HEARTBEAT	User synchronization acknowledgment packet the access device sent to the portal authentication server.
NTF_CHALLENGE	Challenge request packet the access device sent to the portal authentication server.
NTF_USER_NOTIFY	User information notification packet the access device sent to the portal authentication server.
AFF_NTF_USER_NOTIFY	NTF_USER_NOTIFY acknowledgment packet the portal authentication server sent to the access device.

Related commands

`reset portal packet statistics`

display portal rule

Use **`display portal rule`** to display portal filtering rules.

Syntax

`display portal rule` { **`all`** | **`dynamic`** | **`static`** } **`interface`** *`interface-type interface-number`* [**`slot`** *`slot-number`*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

`all`: Displays all portal filtering rules, including dynamic and static portal filtering rules.

`dynamic`: Displays dynamic portal filtering rules, which are generated after users pass portal authentication. These rules allow packets with specific source IP addresses to pass the interface.

`static`: Displays static portal filtering rules, which are generated after portal authentication is enabled. The interface filters packets by these rules when portal authentication is enabled.

interface *interface-type interface-number*: Specifies an interface by its type and number.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays portal filtering rules for all member devices.

Examples

Display all portal filtering rules on VLAN-interface 100.

```
<Sysname> display portal rule all interface vlan-interface 100 slot 1
Slot 1:
IPv4 portal rules on Vlan-interface100:
Rule 1:
 Type               : Static
 Action             : Permit
 Protocol           : Any
 Status             : Active
 Source:
    IP            : 0.0.0.0
    Mask          : 0.0.0.0
    Port          : Any
    MAC           : 0000-0000-0000
    Interface     : Vlan-interface100
    VLAN          : 100
 Destination:
    IP            : 192.168.0.111
    Mask          : 255.255.255.255
    Port          : Any

Rule 2:
 Type               : Dynamic
 Action             : Permit
 Status             : Active
 Source:
    IP            : 2.2.2.2
    MAC           : 000d-88f8-0eab
    Interface     : Vlan-interface100
    VLAN          : 100
 Author ACL:
    Number        : 3001

Rule 3:
 Type               : Static
 Action             : Redirect
 Status             : Active
 Source:
    IP            : 0.0.0.0
    Mask          : 0.0.0.0
    Interface     : Vlan-interface100
    VLAN          : 100
    Protocol      : TCP
```

```
 Destination:
    IP             : 0.0.0.0
    Mask           : 0.0.0.0
    Port           : 80

Rule 4:
 Type               : Static
 Action             : Deny
 Status             : Active
 Source:
    IP             : 0.0.0.0
    Mask           : 0.0.0.0
    Interface      : Vlan-interface100
    VLAN           : Any
 Destination:
    IP             : 0.0.0.0
    Mask           : 0.0.0.0

IPv6 portal rules on Vlan-interface100:
Rule 1:
 Type               : Static
 Action             : Permit
 Protocol           : Any
 Status             : Active
 Source:
    IP             : ::
    Prefix length  : 0
    Port           : Any
    MAC            : 0000-0000-0000
    Interface      : Vlan-interface100
    VLAN           : 100
 Destination:
    IP              : 3000::1
    Prefix length   : 64
    Port            : Any

Rule 2:
 Type               : Dynamic
 Action             : Permit
 Status             : Active
 Source:
    IP             : 3000::1
    MAC            : 0015-e9a6-7cfe
    Interface      : Vlan-interface100
    VLAN           : 100
 Author ACL:
    Number         : 3001
```

```
Rule 3:
 Type                 : Static
 Action               : Redirect
 Status               : Active
 Source:
    IP              : ::
    Prefix length   : 0
    Interface       : Vlan-interface100
    VLAN            : 100
    Protocol        : TCP
 Destination:
    IP              : ::
    Prefix length   : 0
    Port            : 80

Rule 4:
 Type                 : Static
 Action               : Deny
 Status               : Active
 Source:
    IP             : ::
    Prefix length  : 0
    Interface      : Vlan-interface100
    VLAN           : 100
 Destination:
    IP             : ::
    Prefix length  : 0
Author ACL:
    Number          : 3001
```

Table 3 Command output

Field	Description
Rule	Number of the portal filtering rule. IPv4 portal filtering rules and IPv6 portal filtering rules are numbered separately.
Type	Type of the portal filtering rule: • **Static**—Static portal filtering rule. • **Dynamic**—Dynamic portal filtering rule.
Action	Action triggered by the portal filtering rule: • **Permit**—The interface allows packets to pass. • **Redirect**—The interface redirects packets. • **Deny**—The interface forbids packets to pass.
Protocol	Transport layer protocol permitted by the portal-free rule: • **Any**—Permits any transport layer protocol. • **TCP**—Permits TCP. • **UDP**—Permits UDP.
Status	Status of the portal filtering rule: • **Active**—The portal filtering rule is effective. • **Deactive**—The portal filtering rule is not activated.

Source	Source information of the portal filtering rule.
IP	Source IP address.
Mask	Subnet mask of the source IPv4 address.
Prefix length	Prefix length of the source IPv6 address.
Port	Source transport layer port number.
MAC	Source MAC address.
Interface	Layer 2 or Layer 3 interface on which the portal filtering rule is implemented.
VLAN	Source VLAN ID.
Protocol	Transport layer protocol permitted by the portal redirect rule. This field always displays **TCP**.
Destination	Destination information of the portal filtering rule.
IP	Destination IP address.
Port	Destination transport layer port number.
Mask	Subnet mask of the destination IPv4 address.
Prefix length	Prefix length of the destination IPv6 address.
Author ACL	Authorized ACL assigned to authenticated portal users. This field is displayed only for a dynamic portal filtering rule.
Number	Number of the authorized ACL. This field displays **N/A** if the AAA server does not assign an ACL.

display portal server

Use **display portal server** to display information about portal authentication servers.

Syntax

display portal server [*server-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

server-name: Specifies a portal authentication server by its name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

If you do not specify the *server-name* argument, this command displays information about all portal authentication servers.

Examples

Display information about the portal authentication server **pts**.

```
<Sysname> display portal server pts
Portal server: pts
```

```
Type                 : IMC
IP                   : 192.168.0.111
VPN instance         : Not configured
Port                 : 50100
Server detection     : Timeout 60s  Action: log
User synchronization : Timeout 200s
Status               : Up
```

Table 4 Command output

Field	Description
Type	Portal authentication server type: • **CMCC**—CMCC server. • **IMC**—IMC server.
Portal server	Name of the portal authentication server.
IP	IP address of the portal authentication server.
VPN instance	This field is not supported in the current software version. MPLS L3VPN instance where the portal authentication server resides.
Port	Listening port on the portal authentication server.
Server detection	Parameters for portal authentication server detection: • Detection timeout in seconds. • Action (**log**) triggered by the reachability status change of the portal authentication server.
User synchronization	User idle timeout in seconds for portal user synchronization.

Status	Reachability status of the portal authentication server:
	• **Up**—This value indicates one of the following conditions:
	  ○ Portal authentication server detection is disabled.
	  ○ Portal authentication server detection is enabled and the server is reachable.
	• **Down**—Portal authentication server detection is enabled and the server is unreachable.

Related commands

portal enable

portal server

server-detect (portal authentication server view)

user-sync

display portal user

Use **display portal user** to display information about portal users.

Syntax

display portal user { **all** | **interface** *interface-type interface-number* | **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

all: Displays information about all portal users.

interface *interface-type interface-number*: Displays information about portal users on the specified interface.

ip *ipv4-address*: Specifies the IPv4 address of a portal user.

ipv6 *ipv6-address*: Specifies the IPv6 address of a portal user.

verbose: Displays detailed information about portal users.

Examples

Display information about all portal users.

```
<Sysname> display portal user all
Total portal users: 2
Username: abc
  Portal server: pts
  State: Online
  VPN instance: N/A
  MAC               IP                VLAN   Interface
  000d-88f8-0eab    2.2.2.2           100    Vlan-interface100
  Authorization information:
    DHCP IP pool: N/A
    User profile: N/A
    Session group profile: N/A
    ACL number: N/A
    Inbound CAR: N/A
    Outbound CAR: N/A

Username: def
  Portal server: pts
  State: Online
  VPN instance: N/A
  MAC               IP                VLAN   Interface
  000d-88f8-0eac    3.3.3.3           200    Vlan-interface200
  Authorization information:
    DHCP IP pool: N/A
    User profile: N/A
    Session group profile: N/A
    ACL number: 3001
    Inbound CAR: N/A
    Outbound CAR: N/A
```

Table 5 Command output

Field	Description
Total portal users	Total number of portal users.
Username	Name of the user.
Portal server	Name of the portal authentication server.
State	Current state of the portal user: • **Initialized**—The user is initialized and ready for authentication. • **Authenticating**—The user is being authenticated. • **Waiting SetRule**—The user is waiting for authorization information. • **Authorizing**—The user is being authorized. • **Online**—The user is online. • **Waiting Traffic**—The last traffic of the user is to be collected. • **Stop Accounting**—Accounting for the user is stopped. • **Done**—The user goes offline successfully.
VPN instance	This field is not supported in the current software version. MPLS L3VPN instance to which the portal user belongs. If the portal user is on a public network, this field displays **N/A**.
MAC	MAC address of the portal user.
IP	IP address of the portal user.
VLAN	VLAN where the portal user resides.
Interface	Access interface of the portal user.
Authorization information	Authorization information for the portal user.
DHCP IP pool	Name of the authorized IP address pool. If no IP address pool is authorized for the portal user, this field displays **N/A**.
User profile	Authorized user profile: • **N/A**—No user profile is authorized. • **active**—The authorized user profile is applied to the user access interface successfully. • **inactive**—The authorized user profile is not applied to the user access interface or the user profile does not exist on the device.
Session group profile	This field is not supported in the current software version. Authorized session group profile: • **N/A**—No session group profile is authorized. • **active**—The authorized session group profile is applied to the user access interface successfully. • **inactive**—The authorized session group profile is not applied to the user access interface or the session group profile does not exist on the device.
ACL number	Authorized ACL: • **N/A**—No ACL is authorized. • **active**—The authorized ACL is applied to the user access interface successfully. • **inactive**—The authorized ACL is not applied to the user access interface or the ACL does not exist on the device.

Inbound CAR	This field is not supported in the current software version. Authorized inbound CAR: • **CIR**—Committed information rate in bps. • **PIR**—Peak information rate in bps. • **active**—The authorized inbound CAR is applied to the user access interface successfully. • **inactive**—The authorized inbound CAR is not applied to the user access interface. • **N/A**—No inbound CAR is authorized.
Outbound CAR	This field is not supported in the current software version. Authorized outbound CAR: • **CIR**—Committed information rate in bps. • **PIR**—Peak information rate in bps. • **active**—The authorized outbound CAR is applied to the user access interface successfully. • **inactive**—The authorized outbound CAR is not applied to the user access interface. • **N/A**—No outbound CAR is authorized.

Display detailed information about the portal user with IP address 50.50.50.3.

```
<Sysname> display portal user ip 50.50.50.3 verbose
Basic:
  Current IP address: 50.50.50.3
  Original IP address: 30.30.30.2
  Username: user1@hrss
  User ID: 0x18000002
  Access interface: Vlan-interface20
  Service-VLAN/Customer-VLAN: -/-
  MAC address: 0000-0000-0001
  Domain: hrss
  VPN instance: N/A
  Status: Online
  Portal server: test
  Portal authentication method: Direct
AAA:
  Realtime accounting interval: 720s, retry times: 5
  Idle cut: N/A
  Session duration: N/A, remaining: N/A
  Remaining traffic: N/A
  Login time: 2018-01-04 16:13:35 UTC
  Accounting-start fail action: Online
  Accounting-update fail action: Online
  Accounting quota-out action: Offline
  DHCP IP pool: N/A
ACL&QoS&Multicast:
  Inbound CAR: N/A
  Outbound CAR: N/A
  ACL number: 3000 (inactive)
  User profile: N/A
  Session group profile: N/A
```

```
  Max multicast addresses: 4
  Multicast address list: 1.2.3.1, 1.34.33.1, 3.123.123.3, 4.5.6.7
                          2.2.2.2, 3.3.3.3, 4.4.4.4
  User group: 1 (Id=1)
Flow statistic:
  Uplink   packets/bytes: 7/546
  Downlink packets/bytes: 0/0
ITA:
  Accounting merge: Disabled
  Traffic separate: Disabled
  Quota-out offline: Disabled
Level-2 session duration: N/A, remaining: N/A
        Remaining traffic: N/A
        Traffic action: Permit
        Inbound CAR: N/A
        Outbound CAR: N/A
        Uplink packets/bytes: 0/0
        Downlink packets/bytes: 0/0
```

Table 6 Command output

Field	Description
Current IP address	IP address of the portal user after passing authentication.
Original IP address	IP address of the portal user during authentication.
Username	Name of the portal user.
User ID	Portal user ID.
Access interface	Access interface of the portal user.
Service-VLAN/Customer-VLAN	Public VLAN/Private VLAN to which the portal user belongs. If no VLAN is configured for the portal user, this field displays **-/-**.
MAC address	MAC address of the portal user.
Domain	ISP domain name for portal authentication.
VPN instance	This field is not supported in the current software version. MPLS L3VPN instance to which the portal user belongs. If the portal user is on a public network, this field displays **N/A**.
Status	Status of the portal user: • **Authenticating**—The user is being authenticated. • **Authorizing**—The user is being authorized. • **Waiting SetRule**—Deploying portal rules to the user. • **Online**—The user is online. • **Waiting Traffic**—Waiting for traffic from the user. • **Stop Accounting**—Stopping accounting for the user. • **Done**—The user is offline.
Portal server	Name of the portal server.
Portal authentication method	Portal authentication method on the access interface: • **Direct**—Direct authentication.

Field	Description
	• **Re-Dhcp**—Re-DHCP authentication. • **Layer3**—Cross-subnet authentication.
AAA	AAA information about the portal user.
Realtime accounting interval	Interval for sending real-time accounting updates, and the maximum number of accounting attempts. If the real-time accounting is not authorized, this field displays **N/A**.
Idle cut	Idle timeout period and the minimum traffic threshold. If idle cut is not authorized, this field displays **N/A**.
direction	Direction of user traffic: • **Both**—Inbound and outbound traffic. • **Inbound**—Inbound traffic. • **Outbound**—Outbound traffic.
Session duration	Session duration and the remaining session time. If the session duration is not authorized, this field displays **N/A**.
Remaining traffic	Remaining traffic for the portal user. If the remaining traffic is not authorized, this field displays **N/A**.
Login time	Time when the user logged in. The field uses the device time format, for example, 2023-1-19 2:42:30 UTC.
Accounting-start fail action	Action to take on the user when the user encounters accounting-start failure: • **Online**—Allow the user to stay online. • **Offline**—Log out the user.
Accounting-update fail action	Action to take on the user when the user encounters accounting-update failure: • **Online**—Allow the user to stay online. • **Offline**—Log out the user.
Accounting quota-out action	Action to take on the user when the data quotas of the user are used up: • **Online**—Allow the user to stay online. • **Offline**—Log out the user.
DHCP IP pool	Authorized DHCP IP address pool. If no DHCP IP address pool is authorized for the portal user, this field displays **N/A**.
Inbound CAR	This field is not supported in the current software version. Authorized inbound CAR: • **CIR**—Committed information rate in bps. • **PIR**—Peak information rate in bps. • **active**—The authorized inbound CAR is applied to the user access interface successfully. • **inactive**—The authorized inbound CAR is not applied to the user access interface. • **N/A**—No inbound CAR is authorized.
Outbound CAR	This field is not supported in the current software version. Authorized outbound CAR: • **CIR**—Committed information rate in bps. • **PIR**—Peak information rate in bps. • **active**—The authorized outbound CAR is applied to the user access interface successfully. • **inactive**—The authorized outbound CAR is not applied to the user access interface.

Field	Description
	• **N/A**—No outbound CAR is authorized.
ACL number	Authorized ACL: • **N/A**—No ACL is authorized. • **active**—The authorized ACL is applied to the user access interface successfully. • **inactive**—The authorized ACL is not applied to the user access interface or the ACL does not exist on the device.
User profile	Authorized user profile: • **N/A**—No user profile is authorized. • **active**—The authorized user profile is applied to the user access interface successfully. • **inactive**—The authorized user profile is not applied to the user access interface or the user profile does not exist on the device.
Session group profile	This field is not supported in the current software version. Authorized session group profile: • **N/A**—No session group profile is authorized. • **active**—The authorized session group profile is applied to the user access interface successfully. • **inactive**—The authorized session group profile is not applied to the user access interface or the session group profile does not exist on the device.
Max multicast addresses	Maximum number of multicast groups the portal user can join.
Multicast address list	Multicast group list the portal user can join. If no multicast group is authorized, this field displays **N/A**.
User group	Name of the group where the portal user belongs. This field is invalid if the ID is 0xffffffff.
Flow statistic	Flow statistics for the portal user.
Uplink packets/bytes	Packet and byte statistics of the upstream traffic.
Downlink packets/bytes	Packet and byte statistics of the downstream traffic.
ITA	This field is not supported in the current software version. ITA traffic statistics for the portal user.
Accounting merge	This field is not supported in the current software version. Status of the accounting merge feature: • **Enabled**—The accounting merge feature is enabled. The device merges the ITA traffic of all accounting rates in the ITA policy, and applies the lowest rate to the merged traffic. • **Disabled**—The accounting merge feature is disabled. The device sends separate traffic statistics for each accounting rate to the server.
Traffic separate	This field is not supported in the current software version. Whether to exclude the amount of ITA traffic from the overall traffic statistics sent to the accounting server: • **Enabled**—ITA traffic is excluded from the overall traffic statistics. • **Disabled**—ITA traffic is included in the overall traffic statistics.
Quota-out offline	This field is not supported in the current software version. Whether to prohibit the portal user from accessing the authorized IP

Field	Description
	subnets when the user has used up its ITA data quota: • **Enabled**—User cannot access the authorized IP subnets after its ITA data quota is used up. • **Disabled**—User can access the authorized IP subnets after its ITA data quota is used up.
Level-*n* session duration	This field is not supported in the current software version. Authorized level *n* session duration and the remaining session duration. Level *n* represents the accounting level of the portal user in ITA. If the session duration is not authorized, this field displays **N/A**.
Remaining traffic	This field is not supported in the current software version. Remaining ITA traffic for the portal user.
Traffic action	This field is not supported in the current software version. Action for traffic destined for the authorized IP subnets when the portal user has used up its ITA data quota: • **Permit**—Permits traffic destined for the authorized IP subnets. • **Deny**—Denies traffic destined for the authorized IP subnets.
Inbound CAR	This field is not supported in the current software version. Authorized inbound CAR for ITA traffic: • **CIR**—Committed information rate in bps. • **PIR**—Peak information rate in bps. • **active**—The authorized inbound CAR is applied to the user access interface successfully. • **inactive**—The authorized inbound CAR is not applied to the user access interface. • **N/A**—No inbound CAR is authorized.
Outbound CAR	This field is not supported in the current software version. Authorized outbound CAR for ITA traffic: • **CIR**—Committed information rate in bps. • **PIR**—Peak information rate in bps. • **active**—The authorized outbound CAR is applied to the user access interface successfully. • **inactive**—The authorized outbound CAR is not applied to the user access interface. • **N/A**—No outbound CAR is authorized.
Uplink packets/bytes	This field is not supported in the current software version. Packet and byte statistics of the portal user's upstream ITA traffic.
Downlink packets/bytes	This field is not supported in the current software version. Packet and byte statistics of the portal user's downstream ITA traffic.

Related commands

`portal enable`

display portal web-server

Use **`display portal web-server`** to display information about portal Web servers.

Syntax

`display portal web-server` [*`server-name`*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

server-name: Specifies a portal Web server by its name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

If you do not specify the *server-name* argument, this command displays information about all portal Web servers.

Examples

Display information about portal Web server **wbs**.

```
<Sysname> display portal web-server wbs
Portal Web server: wbs
    Type             : IMC
    URL              : http://www.test.com/portal
    URL parameters   : userurl=http://www.test.com/welcome
                       userip=source-address
    VPN instance     : Not configured
    Server detection : Interval: 120s  Attempts: 5  Action: log
    IPv4 status      : Up
    IPv6 status      : Up
    Captive-bypass   : Disabled
    If-match         : original-url http://2.2.2.2 redirect-url http://192.168.56.2
```

Table 7 Command output

Field	Description
Type	Portal Web server type: • **CMCC**—CMCC server. • **IMC**—IMC server.
Portal Web server	Name of the portal Web server.
URL	URL of the portal Web server.
URL parameters	URL parameters for the portal Web server.
VPN instance	This field is not supported in the current software version. Name of the MPLS L3VPN where the portal Web server resides.
Server detection	Parameters for portal Web server detection: • Detection interval in seconds. • Maximum number of detection attempts. • Action (**log**) triggered by the reachability status change of the portal Web server.

IPv4 status	Current state of the IPv4 portal Web server:
	• **Up**—This value indicates one of the following conditions:
	  ○ Portal Web server detection is disabled.
	  ○ Portal Web server detection is enabled and the server is reachable.
	• **Down**—Portal Web server detection is enabled and the server is unreachable.

IPv6 status	Current state of the IPv6 portal Web server:
	• **Up**—This value indicates one of the following conditions:
	  ○ Portal Web server detection is disabled.
	  ○ Portal Web server detection is enabled and the server is reachable.
	• **Down**—Portal Web server detection is enabled and the server is unreachable.

Captive-bypass	Status of the captive-bypass feature: **Enabled** or **Disabled**.
If-match	Match rules configured for URL redirection. If no match rules are configured, this field displays **Not configured**.

Related commands

portal enable

portal web-server

server-detect (portal Web server view)

display web-redirect rule

Use **display web-redirect rule** to display information about Web redirect rules.

Syntax

display web-redirect rule interface *interface-type interface-number* [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays Web redirect rules for the master device.

Examples

Display all Web redirect rules on VLAN-interface 100.

```
<Sysname> display web-redirect rule interface vlan-interface 100
IPv4 web-redirect rules on vlan-interface 100:
Rule 1:
 Type               : Dynamic
 Action             : Permit
 Status             : Active
 Source:
    IP            : 192.168.2.114
```

```
    VLAN           : Any

Rule 2:
 Type               : Static
 Action             : Redirect
 Status             : Active
 Source:
    VLAN           : Any
    Protocol       : TCP
 Destination:
    Port           : 80

IPv6 web-redirect rules on vlan-interface 100:
Rule 1:
 Type               : Static
 Action             : Redirect
 Status             : Active
 Source:
    VLAN           : Any
    Protocol       : TCP
 Destination:
    Port           : 80
```

Table 8 Command output

Field	Description
Rule	Number of the Web redirect rule.
Type	Type of the Web redirect rule: • **Static**—Static Web redirect rule, generated when the Web redirect feature takes effect. • **Dynamic**—Dynamic Web redirect rule, generated when a user visits a redirect webpage.
Action	Action in the Web redirect rule: • **Permit**—Allows packets to pass. • **Redirect**—Redirects the packets.
Status	Status of the Web redirect rule: • **Active**—The Web redirect rule is effective. • **Inactive**—The Web redirect rule is not effective.
Source	Source information in the Web redirect rule.
IP	Source IP address.
Mask	Subnet mask of the source IPv4 address.
Prefix length	Prefix length of the source IPv6 address.
VLAN	Source VLAN. If not specified, this field displays **Any**.
Protocol	Transport layer protocol permitted by the Web redirect rule. This field always displays **TCP**.
Destination	Destination information in the Web redirect rule.
Port	Destination transport layer port number. The default port number is 80.

if-match

Use **if-match** to configure a match rule for URL redirection.

Use **undo if-match** to delete a URL redirection match rule.

Syntax

if-match { **original-url** *url-string* **redirect-url** *url-string* [**url-param-encryption** { **aes** | **des** } **key** { **cipher** | **simple** } *string*] | **user-agent** *string* **redirect-url** *url-string* }

undo if-match { **original-url** *url-string* | **user-agent** *user-agent* }

Default

No URL redirection match rules exist.

Views

Portal Web server view

Predefined user roles

network-admin

Parameters

original-url *url-string*: Specifies a URL string to match the URL in HTTP requests of a portal user. The specified URL must be a complete URL starting with **http://** or **https://**, a case-sensitive string of 1 to 256 characters. The URL string can include question marks (?). If you enter a question mark (?) in the place of the *url-string* argument, the CLI does not display help information for this argument.

redirect-url *url-string*: Specifies the URL to which the user is redirected. The specified URL must be a complete URL starting with **http://** or **https://**, a case-sensitive string of 1 to 256 characters. The URL string can include question marks (?). If you enter a question mark (?) in the place of the *url-string* argument, the CLI does not display help information for this argument.

url-param-encryption: Specifies an encryption algorithm to encrypt the parameters carried in the redirection URL. If you do not specify an encryption algorithm, the parameters carried in the redirection URL are not encrypted.

aes: Specifies the AES algorithm.

des: Specifies the DES algorithm.

key: Specifies a key for encryption.

cipher: Specifies a key in encrypted form.

simple: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the case-sensitive key string. The string length varies by the selected encryption method:

- If **des cipher** is specified, the string length is 41 characters.
- If **des simple** is specified, the string length is 8 characters.
- If **aes cipher** is specified, the string length is 1 to 73 characters.
- If **aes simple** is specified, the string length is 1 to 31 characters.

user-agent *user-agent*: Specifies a user agent string to match the User-Agent string in HTTP or HTTPS requests. The user agent string is a case-sensitive string of 1 to 255 characters. The User-Agent string in HTTP or HTTPS requests includes information about hardware manufacturer, operating system, browser, and search engine.

Usage guidelines

A URL redirection match rule matches HTTP or HTTPS requests by user-requested URL or User-Agent information, and redirects the matching requests to the specified redirection URL.

For a user to successfully access a redirection URL, configure a portal-free rule to allow HTTP or HTTPS requests destined for the redirection URL to pass. For information about configuring portal-free rules, see the **portal free-rule** command.

For a portal Web server, you can configure the **url** command and the **if-match** command for URL redirection. The **url** command redirects all HTTP or HTTPS requests from unauthenticated users to the portal Web server for authentication. The **if-match** command allows for flexible URL redirection by redirecting specific requests to specific redirection URLs. If both commands are executed, the **if-match** command takes priority to perform URL redirection.

Examples

Configure a match rule to redirect HTTP requests destined for the URL **http://www.abc.com.cn** to the URL **http://192.168.0.1** and use **DES** to encrypt the parameters carried in this redirection URL.

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] if-match original-url http://www.abc.com.cn redirect-url
http://192.168.0.1 url-param-encryption des key simple 12345678
```

Configure a match rule to redirect HTTP requests that carry the user agent string **5.0(WindowsNT6.1)AppleWebKit/537.36(KHTML,likeGecko)Chrome/36.0.1985.125Safari/537.36** to the URL **http://192.168.0.1.**

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] if-match user-agent
5.0(WindowsNT6.1)AppleWebKit/537.36(KHTML,likeGecko)Chrome/36.0.1985.125Safari/537.36
redirect-url http://192.168.0.1
```

Related commands

display portal web-server

portal free-rule

url

url-parameter

ip (portal authentication server view)

Use **ip** to specify the IPv4 address of a portal authentication server.

Use **undo ip** to restore the default.

Syntax

ip *ipv4-address* [**key** { **cipher** | **simple** } *string*]

undo ip

Default

The IPv4 address of the portal authentication server is not specified.

Views

Portal authentication server view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies the IPv4 address of the portal authentication server.

key: Specifies a shared key for communication with the portal authentication server. Portal packets exchanged between the access device and the portal authentication server carry an authenticator that is generated with the shared key. The receiver uses the authenticator to check the correctness of the received portal packets.

cipher: Specifies a key in encrypted form.

simple: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. Its plaintext form is a case-sensitive string of 1 to 64 characters. Its encrypted form is a case-sensitive string of 1 to 117 characters.

Usage guidelines

A portal authentication server has only one IPv4 address. Therefore, in portal authentication server view, only one IPv4 address exists. If you execute this command multiple times, the most recent configuration takes effect.

Do not configure the same IPv4 address for different portal authentication servers.

Examples

Specify **192.168.0.111** as the IPv4 address of portal authentication server **pts** and plaintext key **portal** as the shared key for communication with the portal authentication server.

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts] ip 192.168.0.111 key simple portal
```

Related commands

display portal server

portal server

ipv6

Use **ipv6** to specify the IPv6 address of a portal authentication server.

Use **undo ipv6** to restore the default.

Syntax

ipv6 *ipv6-address* [**key** { **cipher** | **simple** } *string*]

undo ipv6

Default

The IPv6 address of the portal authentication server is not specified.

Views

Portal authentication server view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the IPv6 address of the portal authentication server.

key: Specifies a shared key for communication with the portal authentication server. Portal packets exchanged between the access device and the portal authentication server carry an authenticator that is generated with the shared key. The receiver uses the authenticator to check the correctness of the received portal packets.

cipher: Specifies a key in encrypted form.

simple: Specifies a key in plaintext form. For security purposes, the key in plaintext form will be stored in encrypted form.

string: Specifies the key. Its plaintext form is a case-sensitive string of 1 to 64 characters. Its encrypted form is a case-sensitive string of 1 to 117 characters.

Usage guidelines

A portal authentication server has only one IPv6 address. Therefore in portal authentication server view, only one IPv6 address exists. If you execute this command multiple times, the most recent configuration takes effect.

Do not configure the same IPv6 address for different portal authentication servers.

Examples

Specify **2000::1** as the IPv6 address of portal authentication server **pts** and plaintext key **portal** as the shared key for communication with the portal authentication server.

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts] ipv6 2000::1 key simple portal
```

Related commands

display portal server

portal server

port (portal authentication server view)

Use **port** to set the destination UDP port number used by the device to send unsolicited portal packets to the portal authentication server.

Use **undo port** to restore the default.

Syntax

port *port-number*

undo port

Default

The device uses 50100 as the destination UDP port number for unsolicited portal packets.

Views

Portal authentication server view

Predefined user roles

network-admin

Parameters

port-number: Specifies a destination UDP port number the device uses to send unsolicited portal packets to the portal authentication server. The value range for this argument is 1 to 65534.

Usage guidelines

The specified port must be the port that listens to portal packets on the portal authentication server.

Examples

Set the destination UDP port number to **50000** for the device to send unsolicited portal packets to portal authentication server **pts**.

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts] port 50000
```

Related commands

portal server

portal { bas-ip | bas-ipv6 } (interface view)

Use **portal** { **bas-ip** | **bas-ipv6** } to configure the BAS-IP or BAS-IPv6 attribute carried in the portal packets sent to the portal authentication server.

Use **undo portal** { **bas-ip** | **bas-ipv6** } to restore the default.

Syntax

portal { **bas-ip** *ipv4-address* | **bas-ipv6** *ipv6-address* }

undo portal { **bas-ip** | **bas-ipv6** }

Default

The BAS-IP attribute of an IPv4 portal reply packet sent to the portal authentication server is the source IPv4 address of the packet. The BAS-IPv6 attribute of an IPv6 portal reply packet sent to the portal authentication server is the source IPv6 address of the packet.

The BAS-IP attribute of an IPv4 portal notification packet sent to the portal authentication server is the IPv4 address of the packet's output interface. The BAS-IPv6 attribute of an IPv6 portal notification packet sent to the portal authentication server is the IPv6 address of the packet's output interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies BAS-IP for portal packets sent to the portal authentication server. This attribute must be the IPv4 address of an interface on the device. It cannot be 0.0.0.0, 1.1.1.1, a class D address, a class E address, or a loopback address.

ipv6-address: Specifies BAS-IPv6 for portal packets sent to the portal authentication server. This attribute must be the IPv6 address of an interface on the device. It cannot be a multicast address, an all-0 address, or a link-local address.

Usage guidelines

If the device runs Portal 2.0, unsolicited portal packets (such as a logout notification packet) sent to the portal authentication server must carry the BAS-IP attribute. If the device runs Portal 3.0, unsolicited portal packets sent to the portal authentication server must carry the BAS-IP or BAS-IPv6 attribute.

After this command takes effect, the source IP address for unsolicited notification portal packets the device sends to the portal authentication server is the configured BAS IP address. Otherwise, the source IP address of the packets is the IP address of the packet output interface.

You must configure the BAS-IP or BAS-IPv6 attribute on a portal authentication-enabled interface if the following conditions are met:

- The portal authentication server is an H3C IMC server or the portal authentication mode on the interface is re-DHCP.
- The portal device IP address specified on the portal authentication server is not the IP address of the portal packet output interface.

Examples

On interface VLAN-interface 100, configure the BAS-IP attribute as **2.2.2.2** for portal packets sent to the portal authentication server.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname–Vlan-interface100] portal bas-ip 2.2.2.2
```

Related commands

display portal

portal { ipv4-max-user | ipv6-max-user } (interface view)

Use **portal** { **ipv4-max-user** | **ipv6-max-user** } to set the maximum number of portal users allowed on an interface.

Use **undo portal** { **ipv4-max-user** | **ipv6-max-user** } to restore the default.

Syntax

portal { **ipv4-max-user** | **ipv6-max-user** } *max-number*

undo portal { **ipv4-max-user** | **ipv6-max-user** }

Default

The maximum number of portal users allowed on an interface is not limited.

Views

Interface view

Predefined user roles

network-admin

Parameters

max-number: Specifies the maximum number of IPv4 or IPv6 portal users allowed on an interface, in the range of 1 to 4294967295.

Usage guidelines

If the specified maximum number is smaller than the number of current online portal users on the interface, the limit can be set successfully. The limit does not impact the online portal users. However, the device does not allow new portal users to log in from the interface until the number drops down below the limit.

Examples

Set the maximum number of IPv4 portal users to 100 on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
```

```
[Sysname–Vlan-interface100] portal ipv4-max-user 100
```

Related commands

display portal user

portal max-user

portal apply web-server (interface view)

Use **portal** [**ipv6**] **apply web-server** to specify a portal Web server. The device redirects the HTTP requests sent by unauthenticated portal users to the portal Web server.

Use **undo portal** [**ipv6**] **apply web-server** to restore the default.

Syntax

portal [**ipv6**] **apply web-server** *server-name* [**fail-permit** | **secondary**]

undo portal [**ipv6**] **apply web-server** [*server-name*]

Default

No portal Web server is specified.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6: Specifies an IPv6 portal Web server. If the server is an IPv4 portal Web server, do not specify this keyword.

server-name: Specifies a portal Web server by its name, a case-sensitive string of 1 to 32 characters. The name must already exist.

fail-permit: Enables the portal fail-permit feature on the interface. The portal fail-permit feature allows portal users to access the Internet without authentication when the portal Web server is unreachable.

secondary: Specifies the secondary portal Web server. If you do not specify this keyword, this command specifies the primary portal Web server. This keyword is supported only in Release 6348P01 and later.

Usage guidelines

You can enable both IPv4 and IPv6 portal authentication on an interface. Therefore, you can specify both an IPv4 portal Web server and an IPv6 portal Web server on the interface.

When portal fail-permit is enabled for a portal authentication server and a portal Web server on the interface, portal authentication is disabled for users on the interface if either server is unreachable. Portal authentication resumes after both servers become reachable.

For HA, you can specify both a primary portal Web server and a secondary portal Web server. The device preferentially uses the primary portal Web server for portal authentication. If the primary server is unreachable, the device uses the secondary server. Once the primary server becomes reachable, the device forcibly uses the primary server.

To implement automatic primary/secondary server switchover, you must configure server detection for both the primary and secondary portal Web servers.

The fail-permit feature and the secondary portal Web server feature are mutually exclusive. You cannot configure both features for the same server by using this command.

Examples

Specify portal Web server **wbs** on VLAN-interface 100 for portal authentication.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname–Vlan-interface100] portal apply web-server wbs
```

Related commands

display portal

portal fail-permit server

portal web-server

portal authorization strict-checking

Use **portal authorization strict-checking** to enable strict checking on portal authorization information.

Use **undo portal authorization strict-checking** to disable strict checking on portal authorization information.

Syntax

portal authorization { **acl** | **user-profile** } **strict-checking**

undo portal authorization { **acl** | **user-profile** } **strict-checking**

Default

Strict checking on portal authorization information is disabled. If an authorized ACL or user profile does not exist on the device or the user profile fails to be deployed, the user will not be logged out.

Views

Interface view

Predefined user roles

network-admin

Parameters

acl: Enables strict checking on authorized ACLs.

user-profile: Enables strict checking on authorized user profiles.

Usage guidelines

CAUTION:

- The strict checking feature on an interface allows a portal user to stay online only when the authorization information for the user is successfully deployed. The strict checking fails if the authorized ACL or user profile does not exist on the device or the device fails to deploy the user profile.
- You can enable strict checking on the authorized ACL, authorized user profile, or both. If you enable both strict ACL checking and user profile checking, the user will be logged out if either checking fails.

Examples

Enable strict checking on authorized ACLs on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
```

```
[Sysname-Vlan-interface100] portal authorization acl strict-checking
```

Related commands

display portal

portal delete-user

Use **portal delete-user** to log out online portal users.

Syntax

portal delete-user { *ipv4-address* | **all** | **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }

Views

System view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies the IP address of an IPv4 online portal user.

all: Specifies IPv4 and IPv6 online portal users on all interfaces.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you specify this option, this command logs out all IPv4 and IPv6 online portal users on the interface.

ipv6 *ipv6-address*: Specifies the IP address of an IPv6 online portal user.

Examples

Log out the online portal user whose IP address is **1.1.1.1**.

```
<Sysname> system-view
[Sysname] portal delete-user 1.1.1.1
```

Related commands

display portal user

portal device-id

Use **portal device-id** to specify the device ID.

Use **undo portal device-id** to restore the default.

Syntax

portal device-id *device-id*

undo portal device-id

Default

A device is not configured with a device ID.

Views

System view

Predefined user roles

network-admin

Parameters

device-id: Specifies a device ID for the device, a case-sensitive string of 1 to 63 characters.

Usage guidelines

The portal authentication server uses device IDs to identify the devices that send protocol packets to the portal server.

Make sure the configured device ID is different than any other access devices communicating with the same portal authentication server.

Examples

Set the device ID of the device to 0002.0010.100.00.

```
<Sysname> system-view
[Sysname] portal device-id 0002.0010.100.00
```

portal domain (interface view)

Use **portal** [**ipv6**] **domain** to specify a portal authentication domain on an interface. All portal users accessing through the interface must use the authentication domain.

Use **undo portal** [**ipv6**] **domain** to delete the configured portal authentication domain.

Syntax

portal [**ipv6**] **domain** *domain-name*

undo portal [**ipv6**] **domain**

Default

No portal authentication domain is configured on an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6: Specifies an authentication domain for IPv6 portal users. Do not specify this keyword for IPv4 portal users.

domain-name: Specifies an ISP authentication domain by its name, a case-insensitive string of 1 to 255 characters.

Usage guidelines

You can specify both an IPv4 portal authentication domain and an IPv6 portal authentication domain on an interface.

Do not specify the **ipv6** keyword for IPv4 portal users.

Examples

Specify the authentication domain as **my-domain** for IPv4 portal users on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname–Vlan-interface100] portal domain my-domain
```

Related commands

display portal

portal enable (interface view)

Use **portal** [**ipv6**] **enable** to enable portal authentication.

Use **undo portal** [**ipv6**] **enable** to disable portal authentication.

Syntax

portal enable method { **direct** | **layer3** | **redhcp** }

portal ipv6 enable method { **direct** | **layer3** }

undo portal [**ipv6**] **enable**

Default

Portal authentication is disabled.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6: Enables IPv6 portal authentication. Do not specify this keyword for IPv4 portal authentication.

method: Specifies an authentication mode:

- **direct**—Direct authentication.
- **layer3**—Cross-subnet authentication.
- **redhcp**—Re-DHCP authentication.

Usage guidelines

To modify the portal authentication mode, first execute the **undo portal** [**ipv6**] **enable** command to disable portal authentication and then execute the **portal** [**ipv6**] **enable** command.

Make sure the device supports IPv6 ACL and IPv6 forwarding before you enable IPv6 portal authentication on the interface.

IPv6 portal authentication does not support the re-DHCP authentication mode.

You can enable both IPv4 and IPv6 portal authentication on an interface.

Examples

Enable direct IPv4 portal authentication on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname–Vlan-interface100] portal enable method direct
```

Related commands

display portal

portal fail-permit server

Use **portal** [**ipv6**] **fail-permit server** to enable the portal fail-permit feature for a portal authentication server on the interface.

Use **undo portal** [**ipv6**] **fail-permit server** to disable the portal fail-permit feature for the portal authentication server.

Syntax

portal [**ipv6**] **fail-permit server** *server-name*

undo portal [**ipv6**] **fail-permit server**

Default

Portal fail-permit is disabled for the portal authentication server.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6: Specifies an IPv6 portal authentication server. Do not specify this keyword for an IPv4 portal authentication server.

server-name: Specifies a portal authentication server by its name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

When portal fail-permit is enabled for a portal authentication server and a portal Web server on an interface, the interface disables portal authentication for portal users if either server is unreachable. Portal authentication resumes on the interface when both servers become reachable. After portal authentication resumes, unauthenticated portal users need to pass authentication to access network resources. Portal users who has passed authentication can continue accessing network resources.

You can enable portal fail-permit for at most one portal authentication server and one portal Web server on an interface.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Enable portal fail-permit for portal authentication server **pts1** on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname–Vlan-interface100] portal fail-permit server pts1
```

Related commands

display portal

portal fail-permit web-server

Use **portal fail-permit web-server** to enable the portal fail-permit feature for portal Web servers on the interface.

Use **undo portal fail-permit web-server** to disable the portal fail-permit feature for portal Web servers.

Syntax

portal [**ipv6**] **fail-permit web-server**

undo portal [**ipv6**] **fail-permit web-server**

Default

Portal fail-permit is disabled for portal Web servers.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6: Specifies IPv6 portal Web servers. Do not specify this keyword for IPv4 portal Web servers.

Usage guidelines

This command is supported only in Release 6348P01 and later.

On an interface enabled with portal fail-permit for a portal authentication server and portal Web servers, portal authentication on the interface is disabled when all portal Web servers are unreachable. For an interface, the device determines that all portal Web servers are unreachable when both the primary and secondary portal Web servers are unreachable.

Portal authentication resumes on the interface when the specified portal authentication server and a minimum of one portal Web server becomes reachable. After portal authentication resumes, unauthenticated portal users need to pass authentication to access network resources. Portal users who have passed authentication can continue accessing network resources.

Examples

Enable portal fail-permit for portal Web servers on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname–Vlan-interface100] portal fail-permit web-server
```

Related commands

display portal

portal fail-permit server

portal free-all except destination

Use **portal free-all except destination** to configure an IPv4 portal authentication destination subnet on an interface.

Use **undo portal free-all except destination** to delete the IPv4 portal authentication destination subnets on the interface.

Syntax

portal free-all except destination *ipv4-network-address* { *mask-length* | *mask* }

undo portal free-all except destination [*ipv4-network-address*]

Default

No IPv4 portal authentication destination subnet is configured on the interface. Portal users must pass portal authentication to access any subnet.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv4-network-address: Specifies an IPv4 portal authentication subnet address.

mask-length: Specifies the subnet mask length for the authentication subnet address, in the range of 0 to 32.

mask: Specifies the subnet mask in dotted decimal format.

Usage guidelines

Portal users on the interface are authenticated when accessing the specified authentication destination subnet (except IP addresses and subnets specified in portal-free rules). The users can access other subnets without portal authentication.

You can configure multiple authentication destination subnets.

If you do not specify the *ipv4-network-address* argument in the **undo portal free-all except destination** command, this command deletes all IPv4 portal authentication destination subnets on the interface.

Re-DHCP authentication does not support authentication destination subnets.

If you configure both an authentication source subnet and an authentication destination subnet on an interface, only the authentication destination subnet takes effect.

Examples

Configure an IPv4 portal authentication destination subnet of **11.11.11.0**/**24** on VLAN-interface 2. Portal users need to pass authentication to access this subnet and can access other subnets without authentication.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname–Vlan-interface2] portal free-all except destination 11.11.11.0 24
```

Related commands

display portal

portal free-rule

Use **portal free-rule** to configure an IP-based portal-free rule.

Use **undo portal free-rule** to delete portal-free rules.

Syntax

portal free-rule *rule-number* { **destination ip** { *ipv4-address* { *mask-length* | *mask* } | **any** } [**tcp** *tcp-port-number* | **udp** *udp-port-number*] | **source ip** { *ipv4-address* { *mask-length* | *mask* } | **any** } [**tcp** *tcp-port-number* | **udp** *udp-port-number*] } * [**interface** *interface-type interface-number*]

portal free-rule *rule-number* { **destination ipv6** { *ipv6-address prefix-length* | **any** } [**tcp** *tcp-port-number* | **udp** *udp-port-number*] | **source ipv6** { *ipv6-address prefix-length* | **any** } [**tcp** *tcp-port-number* | **udp** *udp-port-number*] } * [**interface** *interface-type interface-number*]

undo portal free-rule { *rule-number* | **all** }

Default

No IP-based portal-free rule is configured.

Views

System view

Predefined user roles

network-admin

Parameters

rule-number: Specifies a portal-free rule number. The value range for this argument is 0 to 4294967295.

destination: Specifies the destination information.

source: Specifies the source information.

ip *ipv4-address*: Specifies an IPv4 address for the portal-free rule.

{ *mask-length* | *mask* }: Specifies the subnet mask of the IPv4 address. The value range for the *mask-length* argument is 0 to 32. The *mask* argument is in dotted decimal format.

ipv6 *ipv6-address*: Specifies an IPv6 address for the portal-free rule.

prefix-length: Specifies the prefix length of the IPv6 address, in the range of 0 to 128.

ip any: Represents any IPv4 address.

ipv6 any: Represents any IPv6 address.

tcp *tcp-port-number*: Specifies a TCP port number for the portal-free rule, in the range of 0 to 65535.

udp *udp-port-number*: Specifies a UDP port number for the portal-free rule, in the range of 0 to 65535.

all: Specifies all portal-free rules.

interface *interface-type interface-number*: Specifies a Layer 3 interface on which the portal-free rule takes effect.

Usage guidelines

You can specify both the **source** and **destination** keyword for a portal-free rule. If you specify only one keyword, the other keyword does not act as a filtering criterion.

If you specify both a source port number and a destination port number for a portal-free rule, the two port numbers must belong to the same transport layer protocol.

If you do not specify a Layer 3 interface, the portal-free rule takes effect on all portal-enabled interfaces.

You cannot configure two portal-free rules with the same filtering criteria.

Examples

Configure an IPv4-based portal-free rule:

- Set the rule number to 1.
- Specify the source IP address as 10.10.10.1/24, the destination IP address as 20.20.20.1, and the destination TCP port number as 23.
- Specify the interface where the rule is applied as VLAN-interface 1.

```
<Sysname> system-view
[Sysname] portal free-rule 1 destination ip 20.20.20.1 32 tcp 23 source ip 10.10.10.1 24
interface vlan-interface 1
```

With this rule, users in subnet 10.10.10.1/24 do not need to pass portal authentication on VLAN-interface 1 when they access services provided on TCP port 23 of host 20.20.20.1.

Configure an IPv6-based portal-free rule:

- Set the rule number to 2.
- Specify the source IP address as 2000::1/64, the destination IP address as 2001::1, and the destination TCP port number as 23.
- Specify the interface as VLAN-interface 1.

```
<Sysname> system-view
[Sysname] portal free-rule 2 destination ipv6 2001::1 128 tcp 23 source ipv6 2000::1 64
interface vlan-interface 1
```

With this rule, users in subnet 2000::1/64 do not need to pass portal authentication on VLAN-interface 1 when they access services provided on TCP port 23 of host 2001::1.

Related commands

display portal rule

portal free-rule destination

Use **portal free-rule destination** to configure a destination-based portal-free rule.

Use **undo portal free-rule** to delete portal-free rules.

Syntax

portal free-rule *rule-number* **destination** *host-name*

undo portal free-rule { *rule-number* | **all** }

Default

No destination-based portal-free rule is configured.

Views

System view

Predefined user roles

network-admin

Parameters

rule-number: Specifies a portal-free rule number. The value range for this argument is 0 to 4294967295.

destination: Specifies the destination host.

host-name: Specifies the destination host by its name, a case-insensitive string of 1 to 253 characters. Valid characters are letters, digits, hyphens (-), underscores (_), dots (.), and asterisks (*). The host name string cannot be **i**, **ip**, **ipv**, or **ipv6**.

all: Specifies all portal-free rules.

Usage guidelines

Before you configure destination-based portal-free rules, make sure a DNS server is deployed on the network.

You can configure a host name in one of the following ways:

- **For exact match**—Specify a complete host name. For example, if you configure the host name as **abc.com.cn** in the portal-free rule, only packets that contain the host name **abc.com.cn** match the rule. Packets that carry any other host names (such as **dfabc.com.cn**) do not match the rule.
- **For fuzzy match**—Specify a host name by placing the asterisk (*) wildcard character at the beginning or end of the host name string. For example, if you configure the host name as

abc.com.cn, abc, or ***abc*,** packets that carry the host name ending with **abc.com.cn**, starting with **abc**, or including **abc** match the rule.

- The asterisk (*) wildcard character represents any characters. The device treats multiple consecutive asterisks as one.
- The configured host name cannot contain only asterisks (*).

The fuzzy match feature takes effect only on HTTP or HTTPS requests initiated by Web browsers.

You cannot configure two destination-based portal-free rules with the same destination information. Otherwise the system prompts you that the same rule already exists.

Examples

Configure a destination-based portal-free rule: specify the rule number as **4** and host name as **www.h3c.com**. This rule allows the portal user who sends the HTTP/HTTPS request that carries the host name **www.h3c.com** to access network resources without authentication.

```
<Sysname> system-view
[Sysname] portal free-rule 4 destination www.h3c.com
```

Related commands

display portal rule

portal free-rule source

Use **portal free-rule source** to configure a source-based portal-free rule. The filtering criteria include source MAC address, source interface, and source VLAN.

Use **undo portal free-rule** to delete a specific or all portal-free rules.

Syntax

portal free-rule *rule-number* **source** { **interface** *interface-type interface-number* | **mac** *mac-address* | **vlan** *vlan-id* } *

undo portal free-rule { *rule-number* | **all** }

Default

No source-based portal-free rules exist.

Views

System view

Predefined user roles

network-admin

Parameters

rule-number: Specifies a portal-free rule number. The value range for this argument is 0 to 4294967295.

interface *interface-type interface-number*: Specifies a source interface by its type and number for the portal-free rule.

mac *mac-address*: Specifies a source MAC address for the portal-free rule, in the form of **H-H-H**.

vlan *vlan-id*: Specifies a source VLAN ID for the portal-free rule. This option takes effect only on portal users that access the network through VLAN interfaces.

all: Specifies all portal-free rules.

Usage guidelines

If you specify both the source VLAN and the source Layer 2 interface, the interface must be in the VLAN.

Examples

Configure source-based portal-free rule: specify the rule number as **3**, source MAC address as **1-1-1**, and source VLAN ID as **10**. This rule allows the portal user whose source MAC address is 1-1-1 from VLAN 10 to access network resources without authentication.

```
<Sysname> system-view
[Sysname] portal free-rule 3 source mac 1-1-1 vlan 10
```

Related commands

display portal rule

portal ipv6 free-all except destination

Use **portal ipv6 free-all except destination** to configure an IPv6 portal authentication destination subnet on an interface.

Use **undo portal ipv6 free-all except destination** to delete IPv6 portal authentication destination subnets on the interface.

Syntax

portal ipv6 free-all except destination *ipv6-network-address prefix-length*

undo portal ipv6 free-all except destination [*ipv6-network-address*]

Default

No IPv6 portal authentication destination subnet is configured. Portal users must pass portal authentication to access any IPv6 subnet.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-network-address: Specifies an IPv6 portal authentication destination subnet.

prefix-length: Specifies the prefix length of the IPv6 subnet, in the range of 0 to 128.

Usage guidelines

Portal users on the interface are authenticated when accessing the specified authentication destination subnet (except IP addresses and subnets specified in portal-free rules). The users can access other subnets without portal authentication.

You can configure multiple authentication destination subnets.

If you do not specify the *ipv6-network-address* argument in the **undo portal ipv6 free-all except destination** command, this command deletes all IPv6 portal authentication destination subnets on the interface.

Re-DHCP authentication does not support authentication destination subnets.

If you configure both an authentication source subnet and an authentication destination subnet on an interface, only the authentication destination subnet takes effect.

Examples

Configure an IPv6 portal authentication destination subnet of **1::2/16** on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname–Vlan-interface2] portal ipv6 free-all except destination 1::2 16
```

Related commands

display portal

portal ipv6 layer3 source

Use **portal ipv6 layer3 source** to configure an IPv6 portal authentication source subnet.

Use **undo portal ipv6 layer3 source** to delete IPv6 portal authentication source subnets.

Syntax

portal ipv6 layer3 source *ipv6-network-address prefix-length*

undo portal ipv6 layer3 source [*ipv6-network-address*]

Default

No IPv6 portal authentication source subnet is configured. Portal users from any IPv6 subnet must pass portal authentication.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-network-address: Specifies an IPv6 portal authentication source subnet address.

prefix-length: Specifies the prefix length of the IPv6 address, in the range of 0 to 128.

Usage guidelines

With IPv6 authentication source subnets configured, only packets from IPv6 users on the authentication source subnets can trigger portal authentication. If an unauthenticated IPv6 user is not on any authentication source subnet, the access device discards all the user's packets that do not match any portal-free rule.

If you do not specify the *ipv6-network-address* argument in the **undo portal ipv6 layer3 source** command, this command deletes all IPv6 portal authentication source subnets on the interface.

Only cross-subnet authentication supports authentication source subnets.

If you configure both an authentication source subnet and an authentication destination subnet on an interface, only the authentication destination subnet takes effect.

Examples

Configure an IPv6 portal authentication source subnet of **1::1/16** on VLAN-interface 2. Only portal users from subnet 1::1/16 trigger portal authentication.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname–Vlan-interface2] portal ipv6 layer3 source 1::1 16
```

Related commands

display portal

portal ipv6 free-all except destination

portal ipv6 user-detect

Use **portal ipv6 user-detect** to enable online detection of IPv6 portal users.

Use **undo portal user-detect** to disable online detection of IPv6 portal users.

Syntax

portal ipv6 user-detect type { **icmpv6** | **nd** } [**retry** *retries*] [**interval** *interval*] [**idle** *time*]

undo portal ipv6 user-detect

Default

Online detection of IPv6 portal users is disabled.

Views

Interface view

Predefined user roles

network-admin

Parameters

type: Specifies the detection type.

- **icmpv6**—ICMPv6 detection.
- **nd**—ND detection.

retry *retries*: Sets the maximum number of detection attempts, in the range of 1 to 10. The default value is 3.

interval *interval*: Sets a detection interval in the range of 1 to 1200 seconds. The default interval is 3 seconds.

idle *time*: Sets the user idle timeout in the range of 60 to 3600 seconds. The default idle timeout is 180 seconds. When the timeout expires, online detection of portal users is started.

Usage guidelines

If the device receives no packets from a portal user within the idle time, the device detects the user's online status as follows:

- **ICMPv6 detection**—Sends ICMPv6 requests to the user at configurable intervals to detect the user status.
  - If the device receives a reply within the maximum number of detection attempts, it considers that the user is online and stops sending detection packets. Then the device resets the idle timer and repeats the detection process when the timer expires.
  - If the device receives no reply after the maximum number of detection attempts, the device logs out the user.
- **ND detection**—Sends ND requests to the user and detects the ND entry status of the user at configurable intervals.
  - If the ND entry of the user is refreshed within the maximum number of detection attempts, the device considers that the user is online and stops detecting the user's ND entry. Then the device resets the idle timer and repeats the detection process when the timer expires.

- If the ND entry of the user is not refreshed after the maximum number of detection attempts, the device logs out the user.

Direct authentication and re-DHCP authentication support both ND detection and ICMPv6 detection. Cross-subnet authentication only supports ICMPv6 detection.

If the access device filters out ICMPv6 packets, ICMPv6 detection might fail and result in the logout of portal users. Make sure the access device does not block ICMPv6 packets before you enable ICMPv6 detection on an interface.

Examples

Enable online detection of IPv6 portal users on VLAN-interface 100. Configure the detection type as **ND**, the maximum number of detection attempts as **5**, the detection interval as **10** seconds, and the user idle timeout as **300** seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname–Vlan-interface100] portal ipv6 user-detect type nd retry 5 interval 10 idle 300
```

Related commands

display portal

portal layer3 source

Use **portal layer3 source** to configure an IPv4 portal authentication source subnet.

Use **undo portal layer3 source** to delete IPv4 portal authentication source subnets.

Syntax

portal layer3 source *ipv4-network-address* { *mask-length* | *mask* }

undo portal layer3 source [*ipv4-network-address*]

Default

No IPv4 portal authentication source subnet is configured. Portal users from any IPv4 subnet must pass portal authentication.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv4-network-address: Specifies an IPv4 portal authentication source subnet address.

mask-length: Specifies the subnet mask length of the IPv4 address, in the range of 0 to 32.

mask: Specifies the subnet mask in dotted decimal format.

Usage guidelines

With IPv4 authentication source subnets configured, only packets from IPv4 users on the authentication source subnets can trigger portal authentication. If an unauthenticated IPv4 user is not on any authentication source subnet, the access device discards all the user's packets that do not match any portal-free rule.

If you do not specify the *ipv4-network-address* argument in the **undo portal layer3 source** command, this command deletes all IPv4 portal authentication source subnets on the interface.

Only cross-subnet authentication supports authentication source subnets.

If you configure both an authentication source subnet and an authentication destination subnet on an interface, only the authentication destination subnet takes effect.

Examples

Configure an IPv4 portal authentication source subnet of **10.10.10.0**/**24** on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname–Vlan-interface2] portal layer3 source 10.10.10.0 24
```

Related commands

display portal

portal free-all except destination

portal local-web-server

Use **portal local-web-server** to enable HTTP- or HTTPS-based local portal Web service and enter its view.

Use **undo portal local-web-server** to disable the local portal Web service.

Syntax

portal local-web-server { **http** | **https ssl-server-policy** *policy-name* [**tcp-port** *port-number*] }

undo portal local-web-server { **http** | **https** }

Default

Local portal Web service is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

http: Specifies the HTTP-based local portal Web service, which uses HTTP to exchange authentication information with clients.

https: Specifies the HTTPS-based local portal Web service, which uses HTTPS to exchange authentication information with clients.

ssl-server-policy *policy-name*: Specifies an existing SSL server policy for HTTPS. The policy name is a case-insensitive string of 1 to 31 characters.

tcp-port *port-number*: Specifies the listening TCP port number for the HTTPS-based local portal Web service. The value range for the *port-number* argument is 1 to 65535. The default port number is 443.

Usage guidelines

In the local portal Web service, the access device also acts as the portal Web server and the portal authentication server. No external portal Web server and portal authentication server are needed.

For an interface to use the local portal Web service, the URL of the portal Web server specified for the interface must meet the following requirements:

- The IP address in the URL must be a local IP address on the device.
- The URL must be ended with **/portal/**. For example: **http://1.1.1.1/portal/**.

You cannot delete an SSL server policy by using the **undo ssl server-policy** command when the policy is associated with HTTPS.

To specify a new SSL server policy for HTTPS, first execute the **undo** form of this command to disable the existing HTTPS-based local portal Web service.

When you specify the listening TCP port number for the HTTPS-based local portal Web service, follow these restrictions and guidelines:

- For the HTTPS-based local portal Web service and other services that use HTTPS:
  - If they use the same SSL server policy, they can use the same TCP port number to listen to HTTPS.
  - If they use different SSL server policies, they cannot use the same TCP port number to listen to HTTPS.
- Do not configure the HTTPS listening TCP port number as the port number used by a known protocol (except HTTPS) or other service. For example, do not specify port numbers 80 and 23, which are used by HTTP and Telnet, respectively.
- Do not configure the same TCP port number for HTTP and HTTPS local portal Web services.

Examples

Enable the HTTP-based local portal Web service and enter its view.

```
<Sysname> system-view
[Sysname] portal local-web-server http
[Sysname-portal-local-websvr-http] quit
```

Enable the HTTPS-based local portal Web service and associate SSL server policy **policy1** with the service.

```
<Sysname> system-view
[Sysname] portal local-web-server https ssl-server-policy policy1
[Sysname-portal-local-websvr-https] quit
```

Change the SSL server policy to **policy2**.

```
[Sysname] undo portal local-web-server https
[Sysname] portal local-web-server https ssl-server-policy policy2
[Sysname-portal-local-websvr-https] quit
```

Enable the HTTPS-based local portal Web service. In the service, the associated SSL server policy is **policy1** and the listening port number is 442.

```
<Sysname> system-view
[Sysname] portal local-web-server https ssl-server-policy policy1 tcp-port 442
[Sysname-portal-local-websvr-https] quit
```

Related commands

default-logon-page

portal local-web-server

ssl server-policy

portal log enable

Use **portal log enable** to enable logging for portal user logins and logouts.

Use **undo user log enable** to disable logging for portal user logins and logouts.

Syntax

portal log enable

undo portal log enable

Default

Portal user login and logout logging is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This feature logs information about portal user login and logout events, including the username, IP address, user's MAC address, interface name, VLAN, and reason for login failure. For portal log messages to be sent correctly, you must also configure the information center on the device. For more information about information center configuration, see *Network Management and Monitoring Configuration Guide*.

Examples

Enable logging for portal user logins and logouts.

```
<Sysname> system-view
[Sysname] portal user log enable
```

portal max-user

Use **portal max-user** to set the maximum number of total portal users allowed in the system.

Use **undo portal max-user** to restore the default.

Syntax

portal max-user *max-number*

undo portal max-user

Default

The total number of portal users allowed in the system is not limited.

Views

System view

Predefined user roles

network-admin

Parameters

max-number: Specifies the maximum number of total portal users in the system. The value range for this argument is 1 to 4294967295.

Usage guidelines

If you configure the maximum total number smaller than the number of current online portal users on the device, this command still takes effect. The online users are not affected by this command, but the system forbids new portal users to log in.

This command sets the maximum number of online IPv4 and IPv6 portal users in all.

Make sure the total number of the maximum IPv4 and IPv6 portal users allowed on all interfaces does not exceed the system-allowed maximum number. Otherwise, the exceeding portal users will not be able to log in to the device.

Examples

Set the maximum number of online portal users allowed in the system to **100**.

```
<Sysname> system-view
[Sysname] portal max-user 100
```

Related commands

display portal user

portal { **ipv4-max-user** | **ipv6-max-user** }

portal nas-id-profile

Use **portal nas-id-profile** to specify a NAS-ID profile for an interface.

Use **undo portal nas-id-profile** to restore the default.

Syntax

portal nas-id-profile *profile-name*

undo portal nas-id-profile

Default

No NAS-ID profile is specified for an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

profile-name: Specifies the name of a NAS-ID profile, a case-insensitive string of 1 to 31 characters.

Usage guidelines

A NAS-ID profile defines the binding relationship between VLANs and NAS-IDs. To configure a NAS-ID profile, use the **aaa nas-id profile** command.

Portal access matches only the inner VLAN ID of QinQ packets. For more information about QinQ, see *Layer 2—LAN Switching Configuration Guide*.

If an interface is specified with a NAS-ID profile, the interface prefers to use the bindings defined in the profile.

If no NAS-ID profile is specified for an interface or no matching binding is found in the specified profile, the device uses the device name as the interface NAS-ID.

Examples

Specify NAS-ID profile **aaa** for VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] portal nas-id-profile aaa
```

Related commands

aaa nas-id profile

portal nas-port-id format

Use **portal nas-port-id format** to specify the NAS-Port-Id attribute format.

Use **undo portal nas-port-id format** to restore the default.

Syntax

portal nas-port-id format { **1** | **2** | **3** | **4** }

undo portal nas-port-id format

Default

The format for the NAS-Port-Id attribute is format 2.

Views

System view

Predefined user roles

network-admin

Parameters

1: Uses format 1 for the NAS-Port-Id attribute.

2: Uses format 2 for the NAS-Port-Id attribute.

3: Uses format 3 for the NAS-Port-Id attribute.

4: Uses format 4 for the NAS-Port-Id attribute.

Usage guidelines

The NAS-Port-Id format supported by RADIUS servers varies by vendor. Use this command to specify the format of the NAS-Port-Id attribute in the RADIUS packets sent for portal users to the RADIUS server. The device then automatically constructs a value for the NAS-Port-Id attribute in the specified format to meet the RADIUS server requirements.

Format 1 contains three space-separated strings: *interface-type port-location access-node-id*. Spaces are not allowed within a string.

- The *interface-type* string specifies the interface type of the NAS port. Available options include:
  - **atm**—ATM interface.
  - **eth**—Common Ethernet interface.
  - **trunk**—Ethernet trunk interface.
  - **0**—The interface type information will be reported by the access node to the BRAS.
- The *port-location* string represents the location of the access line on the BRAS. Its format is NAS_slot/NAS_subslot/NAS_port:XPI.XCI.

Field	Description
NAS_slot	Slot number of the BRAS, in the range of 0 to 31.
NAS_subslot	Subslot number of the BRAS, in the range of 0 to 31.
NAS_Port	Port number of the BRAS, in the range of 0 to 63.
XPI.XCI	For ATM interfaces: • XPI is VPI in the range of 0 to 255. • XCI is VCI in the range of 0 to 65535. For Ethernet interfaces or Ethernet trunk interfaces: • XPI is PVLAN in the range of 0 to 4095. This field is

	set to 4096 if there is no PVLAN. • XCI is CVLAN in the range of 0 to 4095. This field is set to 4096 if the user is not assigned to a VLAN as in the situation where the end user device is directly connected to a BRAS port.

For the access node to report its access line information to the BRAS, all fields will be set to 0s except for the XPI and XCI fields.

- The *access-node-id* string specifies the attributes the of BRAS. Its format is AccessNodeIdentifier/ANI_rack/ANI_frame/ANI_slot/ANI_subslot/ANI_port:ANI_XPI.ANI_XCI, in which the :ANI_XPI.ANI_XCI portion is optional.

AccessNodeIdentifier	Identifier description of the access node, a string not longer than 50 characters without spaces.
ANI_rack	Rack number of the access node, in the range of 0 to 15.
ANI_frame	Frame number of the access node, in the range of 0 to 31.
ANI_slot	Slot number of the access node, in the range of 0 to 127.
ANI_subslot	Subslot number of the access node, in the range of 0 to 31.
ANI_port	Port number of the access node, in the range of 0 to 255.
ANI_XPI.ANI_XCI	Optional. This field is mainly used to carry CPE-side service information, identifying the further service type requirement. For example, use this field to identify specific services in a multi-PVC scenario. For ATM interfaces: • ANI_XPI is VPI in the range of 0 to 255. • ANI_XCI is VCI in the range of 0 to 65535. For Ethernet interfaces or Ethernet trunk interfaces: • ANI_XPI is PVLAN in the range of 0 to 4095. This field is set to 4096 if there is no PVLAN. • ANI_XCI is CVLAN in the range of 0 to 4095. This field is set to 4096 if the user is not assigned to a VLAN as in the situation where the end user device is directly connected to a BRAS port.

If the device does not have rack, frame, or subslot information, 0 is padded in the corresponding field.

For ATM interfaces, all fields in the access-node-id string are filled with 0s except for the ANI_XPI and ANI_XCI fields.

- Examples of format 1:

NAS-Port-Id	**Description**
atm 31/31/7:255.65535 0/0/0/0/0/0	The subscriber interface is an ATM interface. The slot number is 31, the BRAS subslot number is 31, the BRAS port number is 7, the VPI is 255, and the VCI is 65535.
eth 31/31/7:1234.2345 0/0/0/0/0/0	The subscriber interface is an Ethernet interface. The slot number is 31, the subslot number is 31, the port number is 7, the PVLAN is 1234, and the CVLAN is 2345. If there is no PVLAN, 1234 will be replaced with 4096.
eth 31/31/7:4096.2345	The subscriber interface is an Ethernet interface. The slot number

guangzhou001/1/31/63/31/127	is 31, the subslot number is 31, the port number is 7, and the VLAN ID is 2345. The access node identifier of the DSLAM is guangzhou001, the rack number is 1, the frame number is 31, the slot number is 63, subslot number is 31, and the port number is 127.
0 0/0/0:4096.1234 guangzhou001/0/31/63/31/127	The 0 and 0/0/0 strings indicate that BRAS does not have access line information and will use the information received from the access node. After receiving access line information from the access node, the BRAS transparently delivers the information or complements the BRAS access link information as configured. For example, the BRAS complements the access line information as eth 31/31/7:4096.1234 guangzhou001/0/31/63/31/127.

Format 2 is SlotID00IfNOVlanID.

- **SlotID**—Slot number, a string of 2 characters.
- **IfNO**—Slot number, a string of 3 characters.
- **VlanID**—VLAN ID, a string of 9 characters.

Format 3 is SlotID00IfNOVlanIDDHCPoption.

- **SlotID**—Slot number, a string of 2 characters.
- **IfNO**—Interface number, a string of 3 characters.
- **VlanID**—VLAN ID, a string of 9 characters.
- **DHCPoption**—DHCP option 82 is appended for IPv4 users and DHCP option 1 is appended for IPv6.

Format 4 is slot=**;subslot=**;port=**;vlanid=**;vlanid2=**.

- For non-VLAN interfaces, the slot=**;subslot=**;port=**;vlanid=0 format is used.
- For interfaces that terminate only the outermost VLAN tag, the slot=**;subslot=**;port=**;vlanid=** format is used.

Examples

Set the format of the NAS-Port-Id attribute to format 1.

```
<Sysname> system-view
[Sysname] portal nas-port-id format 1
```

portal nas-port-type

Use **portal nas-port-type** to configure the NAS-Port-Type attribute carried in outgoing RADIUS requests.

Use **undo portal nas-port-type** to restore the default.

Syntax

portal nas-port-type { **802.11** | **adsl-cap** | **adsl-dmt** | **async** | **cable** | **ethernet** | **g.3-fax** | **hdlc** | **idsl** | **isdn-async-v110** | **isdn-async-v120** | **isdn-sync** | **piafs** | **sdsl** | **sync** | **virtual** | **wireless-other** | **x.25** | **x.75** | **xdsl** }

undo portal nas-port-type

Default

The NAS-Port-Type carried in outgoing RADIUS requests is Ethernet (attribute value 15).

Views

Interface view

Predefined user roles

network-admin

Parameters

802.11: Specifies the NAS port type as Wireless-IEEE 802.11 (attribute value 19).

adsl-cap: Specifies the NAS port type as ADSL-CAP (attribute value 12).

adsl-dmt: Specifies the NAS port type as ADSL-DMT (attribute value 13).

async: Specifies the NAS port type as Async (attribute value 0).

cable: Specifies the NAS port type as Cable (attribute value 17).

ethernet: Specifies the NAS port type as Ethernet (attribute value 15).

g.3-fax: Specifies the NAS port type as G.3 Fax (attribute value 10).

hdlc: Specifies the NAS port type as HDLC Clear Channel (attribute value 7).

idsl: Specifies the NAS port type as IDSL (attribute value 14).

isdn-async-v110: Specifies the NAS port type as ISDN Async V.110 (attribute value 4).

isdn-async-v120: Specifies the NAS port type as ISDN Async V.120 (attribute value 3).

isdn-sync: Specifies the NAS port type as ISDN Sync (attribute value 2).

piafs: Specifies the NAS port type as PIAFS (attribute value 6).

sdsl: Specifies the NAS port type as SDSL (attribute value 11).

sync: Specifies the NAS port type as Sync (attribute value 1).

virtual: Specifies the NAS port type as Virtual (attribute value 5).

wireless-other: Specifies the NAS port type as Wireless-Other (attribute value 18).

x.25: Specifies the NAS port type as X.25 (attribute value 8).

x.75: Specifies the NAS port type as X.75 (attribute value 9).

xdsl: Specifies the NAS port type as xDSL (attribute value 16).

Examples

Configure the NAS-Port-Type carried in outgoing RADIUS requests as SDSL on VLAN-interface 20.

```
<Sysname> system-view
[Sysname] interface vlan-interface 20
[Sysname-Vlan-interface20] portal nas-port-type sdsl
```

portal pre-auth ip-pool

Use **portal** [**ipv6**] **pre-auth ip-pool** to specify a preauthentication IP address pool for portal users.

Use **undo portal** [**ipv6**] **pre-auth ip-pool** to restore the default.

Syntax

portal [**ipv6**] **pre-auth ip-pool** *pool-name*

undo portal [**ipv6**] **pre-auth ip-pool**

Default

No preauthentication IP address pool is specified for portal users.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6: Specifies IPv6 portal users. Do not specify this keyword for IPv4 portal users.

pool-name: Specifies an IP address pool by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You must use this command to specify a preauthentication IP address pool on a portal-enabled interface in the following situation:

- Portal users access the network through a subinterface of the portal-enabled interface.
- The subinterface does not have an IP address.
- Portal users need to obtain IP addresses through DHCP.

DHCP assigns an IP address from the specified IP address pool to a user. Then, the user can use this IP address to perform portal authentication.

The specified IP address pool takes effect when the following requirements are met:

- The direct portal authentication mode is used on the interface.
- The specified IP address pool must have existed and been correctly configured.

Examples

Create IPv4 address pool **abc** for VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname–Vlan-interface100] portal pre-auth ip-pool abc
```

Related commands

dhcp server ip-pool (*Layer 3—IP Services Command Reference*)

display portal

ipv6 dhcp pool (*Layer 3—IP Services Command Reference*)

portal refresh enable

Use **portal refresh** { **arp** | **nd** } **enable** to enable the Rule ARP or ND entry feature for portal clients.

Use **undo portal refresh** { **arp** | **nd** } **enable** to disable the Rule ARP or ND entry feature for portal clients.

Syntax

portal refresh { **arp** | **nd** } **enable**

undo portal refresh { **arp** | **nd** } **enable**

Default

The Rule ARP or ND entry feature is enabled for portal clients.

Views

System view

Predefined user roles

network-admin

Parameters

arp: Enables the Rule ARP entry feature.

nd: Enables the Rule ND entry feature.

Usage guidelines

When the Rule ARP or ND entry feature is enabled for portal clients, ARP or ND entries for portal clients are Rule entries after the clients come online. The Rule ARP or ND entries will not age out and will be deleted immediately after the portal clients go offline.

If portal clients go offline and then try to come online before the ARP or ND entries are relearned for them, the clients will fail the authentication. In this case, disable this feature so that ARP or ND entries are dynamic entries after the clients come online. The dynamic ARP or ND entries are deleted only when they age out.

Enabling or disabling of this feature does not affect existing Rule/dynamic ARP or ND entries for portal users.

Examples

Disable the Rule ARP entry feature for portal clients.

```
<Sysname> system-view
[Sysname] undo portal refresh arp enable
```

portal roaming enable

Use **portal roaming enable** to enable portal roaming.

Use **undo portal roaming enable** to disable portal roaming.

Syntax

portal roaming enable

undo portal roaming enable

Default

Portal roaming is disabled. An online portal user cannot roam in its VLAN.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Portal roaming applies only to portal users that log in from VLAN interfaces.

This command cannot be executed when online users are present on the device.

If portal roaming is enabled, an online portal user can access network resources from any Layer 2 port in its local VLAN. If portal roaming is disabled, the portal user can access network resources only from the Layer 2 port on which it passes authentication.

For portal roaming to take effect, you must disable the Rule ARP or ND entry feature by using the **undo portal refresh** { **arp** | **nd** } **enable** command.

Examples

Enable portal roaming.

```
<Sysname> system-view
[Sysname] portal roaming enable
```

portal server

Use **portal server** to create a portal authentication server and enter its view, or enter the view of an existing portal authentication server.

Use **undo portal server** to delete the specified portal authentication server.

Syntax

portal server *server-name*

undo portal server *server-name*

Default

No portal authentication servers exist.

Views

System view

Predefined user roles

network-admin

Parameters

server-name: Specifies a portal authentication server by its name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

In portal authentication server view, you can configure the following parameters and features for the portal authentication server:

- IP address of the server.
- Destination UDP port number used by the device to send unsolicited portal packets to the portal authentication server.
- Pre-shared key for communication between the access device and the server.
- Server detection feature.

You can configure multiple portal authentication servers for an access device.

Examples

Create portal authentication server **pts** and enter its view.

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts]
```

Related commands

display portal server

portal user-detect

Use **portal user-detect** to enable online detection of IPv4 portal users.

Use **undo portal user-detect** to disable online detection of IPv4 portal users.

Syntax

portal user-detect type { **arp** | **icmp** } [**retry** *retries*] [**interval** *interval*] [**idle** *time*]

undo portal user-detect

Default

Online detection of IPv4 portal users is disabled.

Views

Interface view

Predefined user roles

network-admin

Parameters

type: Specifies the detection type.

- **arp**—ARP detection.
- **icmp**—ICMP detection.

retry *retries*: Sets the maximum number of detection attempts, in the range of 1 to 10. The default value is 3.

interval *interval*: Sets a detection interval in the range of 1 to 1200 seconds. The default interval is 3 seconds.

idle *time*: Sets a user idle timeout in the range of 60 to 3600 seconds. The default idle timeout is 180 seconds. When the timeout expires, online detection of IPv4 portal users is started.

Usage guidelines

If the device receives no packets from a portal user within the configured idle time, the device detects the user's online status as follows:

- **ICMP detection**—Sends ICMP requests to the user at configurable intervals to detect the user status.
  - If the device receives a reply within the maximum number of detection attempts, it considers that the user is online and stops sending detection packets. Then the device resets the idle timer and repeats the detection process when the timer expires.
  - If the device receives no reply after the maximum number of detection attempts, the device logs out the user.
- **ARP detection**—Sends ARP requests to the user and detects the ARP entry status of the user at configurable intervals.
  - If the ARP entry of the user is refreshed within the maximum number of detection attempts, the device considers that the user is online and stops detecting the user's ARP entry. Then the device resets the idle timer and repeats the detection process when the timer expires.
  - If the ARP entry of the user is not refreshed after the maximum number of detection attempts, the device logs out the user.

Direct authentication and re-DHCP authentication support both ARP detection and ICMP detection. Cross-subnet authentication only supports ICMP detection.

If the access device filters out ICMP packets, ICMP detection might fail and result in the logout of portal users. Make sure the access device does not block ICMP packets before you enable ICMP detection on an interface.

Examples

Enable online detection of IPv4 portal users on VLAN-interface 100. Configure the detection type as **ARP**, the maximum number of detection attempts as **5**, the detection interval as **10** seconds, and the user idle timeout as **300** seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname–Vlan-interface100] portal user-detect type arp retry 5 interval 10 idle 300
```

Related commands

display portal

portal user-dhcp-only (interface view)

Use **portal user-dhcp-only** to allow only users with DHCP-assigned IP addresses to pass portal authentication.

Use **undo portal user-dhcp-only** to restore the default.

Syntax

portal [**ipv6**] **user-dhcp-only**

undo portal [**ipv6**] **user-dhcp-only**

Default

Both users with DHCP-assigned IP addresses and users with static IP addresses can pass portal authentication to come online.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6: Specifies IPv6 portal users. Do not specify this keyword for IPv4 portal users.

Usage guidelines

CAUTION:

- With this feature enabled, users with static IP addresses cannot pass portal authentication to get online.
- To ensure that IPv6 users can pass portal authentication when this feature is enabled, disable the temporary IPv6 address feature. Otherwise, IPv6 users will use temporary IPv6 addresses to access the IPv6 network and will fail portal authentication.

Examples

Allow only users with DHCP-assigned IP addresses on VLAN-interface 100 to pass portal authentication.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname–Vlan-interface100] portal user-dhcp-only
```

Related commands

display portal

portal user-rule assign-check enable

Use **portal user-rule assign-check enable** to enable the device to check the issuing of category-2 portal filtering rules.

Use **undo portal user-rule assign-check enable** to disable the device from checking the issuing of category-2 portal filtering rules.

Syntax

portal user-rule assign-check enable

undo portal user-rule assign-check enable

Default

The device does not check the issuing of category-2 portal filtering rules.

Views

System view

Predefined user roles

network-admin

Usage guidelines

To display category-2 portal filtering rules, use the **display portal rule dynamic** command.

Examples

Enable the device to check the issuing of category-2 portal filtering rules.

```
<Sysname> system-view
[Sysname] portal rule assign-check enable
```

Related commands

display portal rule

portal web-proxy port

Use **portal web-proxy port** to specify the port number of a Web proxy server.

Use **undo portal web-proxy port** to delete port numbers of Web proxy servers.

Syntax

portal web-proxy port *port-number*

undo portal web-proxy port { *port-number* | **all** }

Default

No port numbers of Web proxy servers are specified. Proxied HTTP requests are dropped.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies the port number of a Web proxy server. The value range for this argument is 1 to 65535.

all: Specifies all port numbers of Web proxy servers.

Usage guidelines

To allow HTTP requests proxied by a Web proxy server to trigger portal authentication, specify the port number of the Web proxy server on the device. If a Web proxy server port is not specified on the device, HTTP requests proxied by the Web proxy server are dropped, and portal authentication cannot be triggered.

You can configure this command multiple times to specify multiple port numbers of Web proxy servers.

If a user's browser uses the Web Proxy Auto-Discovery (WPAD) protocol to discover Web proxy servers, you must perform the following tasks on the device:

- Specify the port numbers of the Web proxy servers on the device.
- Configure portal-free rules to allow user packets destined for the IP address of the WPAD server to pass without authentication.

If portal users enable Web proxy in their browsers, the users must add the IP address of the portal authentication server as a proxy exception in their browsers. Then, HTTP packets that the users send to the portal authentication server will not be sent to Web proxy servers.

You cannot specify Web proxy server port 443 on the device.

Examples

Specify Web proxy server port 8080.

```
<Sysname> system-view
[Sysname] portal web-proxy port 8080
```

Related commands

portal enable method

portal web-server

Use **portal web-server** to create a portal Web server and enter its view, or enter the view of an existing portal Web server.

Use **undo portal web-server** to delete a portal Web server.

Syntax

portal web-server *server-name*

undo portal web-server *server-name*

Default

No portal Web servers exist.

Views

System view

Predefined user roles

network-admin

Parameters

server-name: Specifies a portal Web server by its name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

The portal Web server pushes portal authentication pages to portal users during authentication. The access device redirects HTTP requests of unauthenticated portal users to the portal Web server. In portal Web server view, you can configure the URL and URL parameters for the portal Web server and the portal Web server detection feature.

Examples

Create portal Web server **wbs** and enter its view.

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs]
```

Related commands

display portal web-server

portal apply web-server

reset portal packet statistics

Use **reset portal packet statistics** to clear packet statistics for portal authentication servers.

Syntax

reset portal packet statistics [**server** *server-name*]

Views

User view

Predefined user roles

network-admin

Parameters

server-name: Specifies a portal authentication server by its name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

If you do not specify the **server** *server-name* option, this command clears packet statistics for all portal authentication servers.

Examples

Clear packet statistics for portal authentication server **pts**.

```
<Sysname> reset portal packet statistics server pts
```

Related commands

display portal packet statistics

server-detect (portal authentication server view)

Use **server-detect** to enable portal authentication server detection. After server detection is enabled for a portal authentication server, the device periodically detects portal packets from the server to identify its reachability status.

Use **undo server-detect** to disable portal authentication server detection.

Syntax

server-detect [**timeout** *timeout*] **log**

undo server-detect

Default

Portal authentication server detection is disabled.

Views

Portal authentication server view

Predefined user roles

network-admin

Parameters

timeout *timeout*: Specifies the detection timeout in the range of 10 to 3600 seconds. The default is 60 seconds.

log: Configures the device to send a log message after detecting reachability status change of the portal authentication server. The log message contains the name, the original state, and the current state of the portal authentication server.

Usage guidelines

The portal authentication server detection feature takes effect only when the device has a portal-enabled interface.

To test server reachability by detecting heartbeat packets, you must enable the server heartbeat feature on the portal authentication server. Only the IMC portal authentication server supports sending heartbeat packets.

The detection timeout configured on the device must be greater than the server heartbeat interval configured on the portal authentication server.

If the device receives portal packets from the portal authentication server before the detection timeout expires and verifies the correctness of the packets, the device considers the portal authentication server is reachable. Otherwise, the device considers the portal authentication server is unreachable.

Examples

Enable server detection for portal authentication server **pts**:

- Set the detection timeout to 600 seconds.
- Configure the device to send a log message if the server reachability status changes.

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts] server-detect timeout 600 log
```

Related commands

portal server

server-detect (portal Web server view)

Use **server-detect** to enable portal Web server detection.

Use **undo server-detect** to disable portal Web server detection.

Syntax

server-detect [**interval** *interval*] [**retry** *retries*] **log**

undo server-detect

Default

Portal Web server detection is disabled.

Views

Portal Web server view

Predefined user roles

network-admin

Parameters

interval *interval*: Specifies a detection interval in the range of 10 to 1200 seconds. The default is 20 seconds.

retry *retries*: Specifies the maximum number of consecutive detection failures, in the range of 1 to 10. The default is 3. If the number of consecutive failed detections reaches this threshold, the device considers the server as unreachable.

log: Configures the device to send a log message after detecting reachability status change of the portal Web server. The log message contains the name, the original state, and the current state of the portal Web server.

Usage guidelines

The access device performs server detection independently. No configuration on the portal Web server is required for the detection.

The portal Web server detection feature takes effect only when the URL of the portal Web server is specified and the device has a portal-enabled interface.

Examples

Enable server detection for portal Web server **wbs**:

- Set the detection interval to 600 seconds.
- Set the maximum number of consecutive detection failures to 2.
- Configure the device to send a log message after server reachability status changes.

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] server-detect interval 600 retry 2 log
```

Related commands

portal web-server

server-register

Use **server-register** to configure the device to periodically send register packets to the portal authentication server.

Use **undo server-register** to restore the default.

Syntax

server-register [**interval** *interval-value*]

undo server-register

Default

The device does not send register packets to a portal authentication server.

Views

Portal authentication server view

Predefined user roles

network-admin

Parameters

interval *interval-value*: Specifies the interval at which the device sends register packets to the portal authentication server, in seconds. The value range for the *interval* argument is 1 to 3600, and the default value is 600.

Usage guidelines

This feature is typically used in scenarios where a NAT device exists between a portal authentication server and a large number of access devices.

If this feature is disabled, you must configure a static NAT mapping for each access device on the NAT device. If this feature is enabled, the access device automatically sends a register packet to the portal authentication server. When the server receives the register packet, it records register information for the access device, including the device name and the IP address and port number after NAT. The register information is used for subsequent authentication information exchanges between the server and the access device. The access device updates its register information on the server by sending register packets at regular intervals.

This feature can work with only CMCC portal authentication servers.

Examples

Configure the device to send register packets to portal authentication server **pts** at intervals of 120 seconds.

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts] server-register interval 120
```

Related commands

server-type

server-type (portal authentication/Web server view)

Use **server-type** to specify the type of a portal authentication server or portal Web server.

Use **undo server-type** to restore the default.

Syntax

server-type { **cmcc** | **imc** }

undo server-type

Default

The type of the portal authentication server and portal Web server is IMC.

Views

Portal authentication server view

Portal Web server view

Predefined user roles

network-admin

Parameters

cmcc: Specifies the portal server type as CMCC.

imc: Specifies the portal server type as IMC.

Usage guidelines

Specify the portal server type on the device with the server type the device actually uses.

Examples

Specify the type of portal authentication server as **imc**.

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts] server-type imc
```

Specify the type of portal Web server as **imc**.

```
<Sysname> system-view
[Sysname] portal web-server pts
[Sysname-portal-websvr-pts] server-type imc
```

Related commands

display portal server

tcp-port

Use **tcp-port** to configure a listening TCP port for the local portal Web service.

Use **undo tcp-port** to restore the default.

Syntax

tcp-port *port-number*

undo tcp-port

Default

The listening TCP port number for HTTP is 80 and that for HTTPS is the TCP port number set by the **portal local-web-server** command.

Views

Local portal Web service view

Predefined user roles

network-admin

Parameters

port-number: Specifies the listening TCP port number in the range of 1 to 65535.

Usage guidelines

To use the local portal Web service, make sure the port number in the portal Web server URL and the port number configured in this command are the same.

For successful local portal authentication, follow these guidelines:

- Do not configure the listening TCP port number for a local portal Web service as the port number used by a known protocol. For example, do not specify port numbers 21 and 23, which are used by FTP and Telnet, respectively.

- Do not configure the HTTP listening port number as the default HTTPS listening port number 443.
- Do not configure the HTTPS listening port number as the default HTTP listening port number 80.
- Do not configure the same listening port number for HTTP and HTTPS.
- For the HTTPS-based local portal Web service and other services that use HTTPS:
  - If they use the same SSL server policy, they can use the same TCP port number to listen to HTTPS.
  - If they use different SSL server policies, they cannot use the same TCP port number to listen to HTTPS.

Examples

Set the listening port number to 2331 for the HTTP-based local portal Web service.

```
<Sysname> system-view
[Sysname] portal local-web-server http
[Sysname-portal-local-websvr-http] tcp-port 2331
```

Related commands

portal local-web-server

url

Use **url** to specify a URL for a portal Web server.

Use **undo url** to restore the default.

Syntax

url *url-string*

undo url

Default

No URL is specified for a portal Web server.

Views

Portal Web server view

Predefined user roles

network-admin

Parameters

url-string: Specifies a URL for the portal Web server, a case-sensitive string of 1 to 256 characters. The URL string can include question marks (?). If you enter a question mark (?) in the place of the *url-string* argument, the CLI does not display help information for this argument.

Usage guidelines

This command specifies a URL that can be accessed through standard HTTP or HTTPS. The URL should start with **http://** or **https://**. If the URL you specify does not start with **http://** or **https://,** the system considers the URL begins with **http://** by default.

Examples

Configure the URL for portal Web server **wbs** as **http://www.test.com/portal**.

```
<Sysname> system-view
[Sysname] portal web-server wbs
```

```
[Sysname-portal-websvr-wbs] url http://www.test.com/portal
```

Related commands

display portal web-server

url-parameter

Use **url-parameter** to configure the parameters carried in the URL of a portal Web server. The access device redirects a portal user by sending the URL with the parameters to the user.

Use **undo url-parameter** to delete the parameters carried in the URL of the portal Web server.

Syntax

url-parameter *param-name* { **original-url** | **source-address** | **source-mac** [**encryption** { **aes** | **des** } **key** { **cipher** | **simple** } *string*] | **value** *expression* }

undo url-parameter *param-name*

Default

No URL parameters are configured for a portal Web server.

Views

Portal Web server view

Predefined user roles

network-admin

Parameters

param-name: Specifies a URL parameter name, a case-sensitive string of 1 to 32 characters. Content of the parameter is determined by the following keyword you specify.

original-url: Specifies the URL of the original webpage that a portal user visits.

source-address: Specifies the user IP address.

source-mac: Specifies the user MAC address.

encryption: Specifies the encryption algorithm to encrypt the MAC address of the user.

aes: Specifies the AES algorithm.

des: Specifies the DES algorithm.

key: Specifies a key for encryption.

cipher: Specifies a key in encrypted form.

simple: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the case-sensitive key string. The string length varies by the selected encryption method:

- If **des cipher** is specified, the string length is 41 characters.
- If **des simple** is specified, the string length is 8 characters.
- If **aes cipher** is specified, the string length is 1 to 73 characters.
- If **aes simple** is specified, the string length is 1 to 31 characters.

value *expression*: Specifies a custom case-sensitive string of 1 to 256 characters. The string can include question marks (?). If you enter a question mark (?) in the place of the *expression* argument, the CLI does not display help information for this argument.

Usage guidelines

You can configure multiple URL parameters.

If you execute this command multiple times to configure the same URL parameter, the most recent configuration takes effect.

After you configure the URL parameters, the access device sends the portal Web server URL with these parameters to portal users. For example, assume that the URL of a portal Web server is http://www.test.com/portal, and you execute the **url-parameter userip source-address** and **url-parameter userurl value http://www.abc.com/welcome** commands. Then, the access device sends to the user whose IP address is 1.1.1.1 the URL **http://www.test.com/portal?userip=1.1.1.1&userurl=http://www.abc.com/welcome**.

When you configure the *param-name* argument in this command, you must use the URL parameter name supported by the actual portal server. Different portal server types support different URL parameter names.

For example, the IMC server supports parameter names **userurl**, **userip**, and **usermac** for the keywords **original-url**, **source-address**, and **source-mac**, respectively. To carry the user IP information in the portal Web server URL, you must configure the parameter name as **userip** and specify the **source-address** keyword.

If you specify the encryption algorithm for a parameter, the redirection URL carries the encrypted value for the parameter. Execute the **url-parameter usermac source-mac encryption des key simple 12345678** command. Then the access device sends to the user with MAC address 1111-1111-1111 the URL **http://www.test.com/portal?usermac=xxxxxxxxx&userip=1.1.1.1&userurl=http://www.test.com/welcome**, where **xxxxxxxxx** represents the encrypted user MAC address.

Examples

Configure URL parameters **userip** and **userurl** for the portal Web server **wbs**. Configure the value of the **userip** parameter as **source-address** (the IP addresses of users) and that of the **userurl** parameter as **http://www.abc.com/welcome**.

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] url-parameter userip source-address
[Sysname-portal-websvr-wbs] url-parameter userurl value http://www.abc.com/welcome
```

Configure URL parameter **usermac** for the portal Web server **wbs**. Configure the value of the **usermac** parameter as **source-mac** (the MAC addresses of users) and specify DES to encrypt the MAC addresses.

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] url-parameter usermac source-mac encryption des key simple
12345678
```

Related commands

display portal web-server

url

user-sync

Use **user-sync** to enable portal user synchronization for a portal authentication server.

Use **undo user-sync** to disable portal user synchronization for a portal authentication server.

Syntax

user-sync timeout *timeout*

undo user-sync

Default

Portal user synchronization is disabled for a portal authentication server.

Views

Portal authentication server view

Predefined user roles

network-admin

Parameters

timeout *timeout*: Sets a detection timeout for synchronization packets, in the range of 60 to 18000 seconds.

Usage guidelines

After this feature is enabled, the device replies to and periodically detects the synchronization packets from the portal authentication server. In this way, information about online portal users on the device and on the portal authentication server remains consistent.

Portal user synchronization requires that the portal authentication server support the portal user heartbeat feature. Now, only the IMC portal authentication server supports portal user heartbeat. To implement portal user synchronization, you need to configure the user heartbeat feature on the portal authentication server. Make sure the user heartbeat interval configured on the portal authentication server is not greater than the synchronization detection timeout configured on the access device.

Deleting a portal authentication server on the device also deletes the user synchronization configuration for the server.

If you execute this command multiple times, the most recent configuration takes effect.

For information of the users considered as nonexistent on the portal authentication server, the device deletes the information after the configured detection timeout expires.

If the user information from the portal authentication server does not exist on the device, the device encapsulates IP addresses of the users in user heartbeat reply packets to the server. The portal authentication server then deletes the users.

Examples

Enable portal user synchronization for portal authentication server **pts** and set the detection timeout to **600** seconds. If a use has not appeared in the synchronization packets sent by the portal authentication server for 600 seconds, the access device logs out the user.

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts] user-sync timeout 600
```

Related commands

portal server

web-redirect url

Use **web-redirect url** to enable the Web redirect feature.

Use **undo web-redirect url** to disable the Web redirect feature.

Syntax

web-redirect [**ipv6**] **url** *url-string* [**interval** *interval*]

undo web-redirect [**ipv6**]

Default

The Web redirect feature is disabled.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6: Specifies the IPv6 Web redirect feature. Do not specify this keyword for the IPv4 Web redirect feature.

url *url-string*: Specifies the URL to which the user is redirected. The URL is required to be complete and begins with **http://** or **https://**, a string of 1 to 256 characters. The URL string can include question marks (?). If you enter a question mark (?) in the place of the *url-string* argument, the CLI does not display help information for this argument.

interval *interval*: Specifies the time interval at which the user is redirected to the specified URL. It is in the range of 60 to 86400 seconds. The default interval is 86400 seconds.

Usage guidelines

With Web redirect enabled on an interface, a user on the interface is first redirected to the specified URL before the user can access an external network through a Web browser. After the specified interval, the user is redirected to the specified URL again.

Web redirect does not work when both Web redirect and portal authentication are enabled.

The Web redirect feature takes effect only on HTTP packets that use the default port number 80.

Examples

Configure IPv4 Web redirect on VLAN-interface 100. Set the redirect URL to **http://192.0.0.1** and the interval to **3600** seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname–Vlan-interface100] web-redirect url http://192.0.0.1 interval 3600
```

Related commands

display web-redirect rule

Contents

Web authentication commands

display web-auth

Use **display web-auth** to display Web authentication configuration and running status on interfaces.

Syntax

display web-auth [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays Web authentication configuration for all interfaces.

Examples

Display Web authentication configuration on GigabitEthernet 1/0/1.

```
<Sysname> display web-auth interface gigabitethernet 1/0/1
 Global Web-auth parameters:
   Temp entry aging time     : 500 s
   HTTP proxy port numbers   : Not configured
   HTTPS proxy port numbers  : Not configured
 Total online web-auth users  : 1

 GigabitEthernet1/0/1  is link-up
   Port role               : Authenticator
   Web-auth domain          : my-domain
   Auth-Fail VLAN           : Not configured
   Offline-detect           : Not configured
   Max online users         : 1024
   Web-auth enable          : Enabled

   Total online web-auth users: 1
```

Table 1 Command output

Field	Description
Global Web-auth parameters	Global Web authentication configuration.
Temp entry aging time	Aging timer for temporary MAC address entries. This field is supported only in Release 6343P08 and later.
HTTP proxy port numbers	HTTP port numbers of the Web proxy servers.
HTTPS proxy port numbers	HTTPS port numbers of the Web proxy servers.

Total online web-auth users	Total number of online Web authentication users on the device.
GigabitEthernet1/0/1 is link-up	State of the interface: • **link-up**—The interface is both administratively and physically up. • **link-down**—The interface is down.
Port role	Role of the port. The port functions only as an **Authenticator**.
Web-auth domain	ISP domain used by Web authentication.
Auth-fail VLAN	Auth-Fail VLAN for Web authentication. This field displays **Not configured** if no Auth-Fail VLAN is configured.
Offline-detect	Interval of Web authentication user detection. This field displays **Not configured** if online detection for Web authentication users is disabled.
Max online users	Maximum number of Web authentication users allowed on the interface.
Web-auth enable	State of Web authentication: • Enabled. • Disabled.
Total online web-auth users	Total number of online Web authentication users on the interface.

display web-auth free-ip

Use **display web-auth free-ip** to display Web authentication-free subnets.

Syntax

display web-auth free-ip

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display Web authentication-free subnets.

```
<Sysname> display web-auth free-ip
      Free IP
                      : 1.1.0.0       255.255.0.0
                      : 1.2.0.0       255.255.0.0
```

Related commands

web-auth free-ip

display web-auth server

Use **display web-auth server** to display Web authentication server information.

Syntax

display web-auth server [*server-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

server-name: Specifies a Web authentication server name, a case-sensitive string of 1 to 32 characters. If you do not specify a Web authentication server, this command displays information about all Web authentication servers.

Examples

Display information about Web authentication server **aaa**.

```
<Sysname> display web-auth server aaa
Web-auth server: aaa
  IP                   : 8.8.8.8
  Port                 : 80
  URL                  : http://8.8.8.8/portal/
  Redirect-wait-time   : 5
  URL parameters       : Not configured
```

Table 2 Command output

Field	Description
Web-auth server	Name of the Web authentication server.
IP	IP address of the Web authentication server.
Port	Port number of the Web authentication server.
URL	Redirection URL of the Web authentication server.
Redirect-wait-time	Time before redirecting an authenticated user to the webpage requested by the user.
URL parameters	Parameters in the redirection URL.

display web-auth user

Use **display web-auth user** to display information about online Web authentication users on interfaces.

Syntax

display web-auth user [**interface** *interface-type interface-number* | **slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays information about online Web authentication users on all interfaces.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays online Web authentication user information for all member devices.

Examples

Display information about online Web authentication users on GigabitEthernet 1/0/1.

```
<Sysname> display web-auth user interface gigabitethernet 1/0/1
  Total online web-auth users: 1

User name: user1
  MAC address: 0000-2700-b076
  Access interface: GigabitEthernet 1/0/1
  Initial VLAN: 1
  Authorization VLAN: N/A
  Authorization ACL ID: N/A
  Authorization user profile: N/A
```

Table 3 Command output

Field	Description
Total online web-auth users	Total number of online Web authentication users.
User Name	Name of the online Web authentication user.
MAC address	MAC address of the online Web authentication user.
Access interface	Access interface of the online Web authentication user.
Initial VLAN	Initial VLAN of the user before the user passes Web authentication.
Authorization VLAN	Authorization VLAN ID of the online Web authentication user.
Authorization ACL ID	Authorization ACL number of the online Web authentication user.
Authorization user profile	Status of user profile of the online Web authentication user: • **N/A**—No user profile is authorized. • **Active**—The authorized user profile is applied to the user access interface successfully. • **Inactive**—The authorized user profile is not applied to the user access interface or the user profile does not exist on the device.

ip

Use **ip** to specify the IP address and port number for a Web authentication server.

Use **undo ip** to restore the default.

Syntax

ip *ipv4-address* **port** *port-number*

undo ip

Default

No IP address or port number is specified for a Web authentication server.

Views

Web authentication server view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies the IPv4 address of the Web authentication server. This IP address is that of a Layer 3 interface on the access device and must be routable to and from the Web authentication user.

port *port-number*: Specifies the port number of the Web authentication server, in the range of 1 to 65535.

User guidelines

As a best practice, use the IP address of a loopback interface as the IP address of the Web authentication server. A loopback interface has the following advantages:

- The status of a loopback interface is stable. This can avoid authentication page access failures caused by interface failures.
- A loopback interface does not forward received packets. This can avoid impacting system performance when there are many network access requests.

The port number of the Web authentication server must be the same as the listening port of the local portal Web service. For more information about the local portal Web service configuration, see portal authentication in *Security Configuration Guide*.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Enter the view of Web authentication server **wbs**.

```
<Sysname> system-view
[Sysname] web-auth server wbs
```

Specify 192.168.1.1 as the IP address and 8080 as the port number for Web authentication server **wbs**.

```
[Sysname-web-auth-server-wbs] ip 192.168.1.1 port 8080
```

Related commands

url

tcp-port

redirect-wait-time

Use **redirect-wait-time** to set the redirection wait time. After a user passes Web authentication, the device waits for the specified period of time before redirecting the user to the specified webpage.

Use **undo redirect-wait-time** to restore the default.

Syntax

redirect-wait-time *period*

undo redirect-wait-time

Default

The redirection wait time is 5 seconds.

Views

Web authentication server view

Predefined user roles

network-admin

Parameters

period: Specifies the redirection wait time in the range of 1 to 90 seconds.

Usage guidelines

After a user passes Web authentication and is assigned an authorization VLAN, the user might need to change the IP address of the authentication client. To ensure that the redirection URL can be successfully opened, set the redirection wait time to be greater than the time that the user takes to update the IP address of the client.

Examples

Set the redirection wait time for authenticated users to 10 seconds.

```
<Sysname> system-view
[Sysname] web-auth server wbs
[Sysname-web-auth-server-wbs] redirect-wait-time 10
```

url

Use **url** to specify the redirection URL for a Web authentication server.

Use **undo url** to restore the default.

Syntax

url *url-string*

undo url

Default

No redirection URL is specified for a Web authentication server.

Views

Web authentication server view

Predefined user roles

network-admin

Parameters

url-string: Specifies the redirection URL for the Web authentication server, a case-sensitive string of 1 to 256 characters. The URL string can include question marks (?). If you enter a question mark (?) in the place of the *url-string* argument, the CLI does not display help information for this argument.

Usage guidelines

The redirection URL is a URL that can be accessed through standard HTTP or HTTPS. The redirection URL should start with **http://** or **https://**. If the redirection URL does not start with http:// or https://, the system determines that the URL begins with **http://**.

The IP address and port number in the URL must be the same as the IP address and port number of the Web authentication server.

Examples

Specify **http://192.168.1.1:80/portal/** as the redirection URL for Web authentication server **wbs**.

```
<Sysname> system-view
[Sysname] web-auth server wbs
[Sysname-web-auth-server-wbs] url http://192.168.1.1:80/portal/
```

Related commands

ip

tcp-port

url-parameter

Use **url-parameter** to add parameters to the redirection URL of Web authentication.

Use **undo url-parameter** to delete parameters from the redirection URL of Web authentication.

Syntax

url-parameter *parameter-name* { **original-url** | **source-address** | **source-mac** | **value** *expression* }

undo url-parameter *parameter-name*

Default

No URL parameters are added to the redirection URL of Web authentication.

Views

Web authentication server view

Predefined user roles

network-admin

Parameters

parameter-name: Specifies a URL parameter name, a case-sensitive string of 1 to 32 characters. Content of the parameter is determined by the following keyword you specify.

original-url: Specifies the URL of the original webpage that a portal user visits.

source-address: Specifies the user IP address.

source-mac: Specifies the user MAC address.

value *expression*: Specifies a custom case-sensitive string of 1 to 256 characters. The string can include question marks (?). If you enter a question mark (?) in the place of the *expression* argument, the CLI does not display help information for this argument.

Usage guidelines

You can repeat this command to add multiple URL parameters to the redirection URL of Web authentication. For example, to add the user IP address and a custom string of **http://www.abc.com/welcome** to the redirection URL, execute the following commands:

- **url-parameter userip source-address**.
- **url-parameter userurl value http://www.abc.com/welcome**.

The device will redirect Web requests from IP address 1.1.1.1 to the URL at **http://192.168.1.1/portal?userip=1.1.1.1&userurl=http://www.abc.com/welcome**.

If you execute this command multiple times to configure the same URL parameter, the most recent configuration takes effect.

When you configure the *parameter-name* argument in this command, you must use the URL parameter name supported by the Web browser. Different Web browsers support different URL parameter names.

Examples

Add parameters **userip** and **userurl** to the redirection URL of portal Web server **wbs**.

```
<Sysname> system-view
[Sysname] web-auth server wbs
[Sysname-web-auth-server-wbs] url-parameter userip source-address
[Sysname-web-auth-server-wbs] url-parameter userurl value http://www.abc.com/welcome
```

Related commands

web-auth server

web-auth auth-fail vlan

Use **web-auth auth-fail vlan** to specify an Auth-Fail VLAN for Web authentication.

Use **undo web-auth auth-fail vlan** to restore the default.

Syntax

web-auth auth-fail vlan *authfail-vlan-id*

undo web-auth auth-fail vlan

Default

No Auth-Fail VLAN is specified for Web authentication.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

authfail-vlan-id: Specifies the Auth-Fail VLAN ID in a range of 1 to 4094. The specified VLAN must already exist.

User guidelines

After you configure this command on an interface, users who failed Web authentication on the interface can access resources in the Auth-Fail VLAN. You must also configure the IP address of the server that provides the resources as an authentication-free IP address.

To make the Auth-Fail VLAN take effect, you must also enable MAC-based VLAN on the interface, and set the subnet of the Auth-Fail VLAN as the Web authentication-free subnet.

Because MAC-based VLAN takes effect only on Hybrid ports, Auth-Fail VLAN also takes effect only on Hybrid ports.

If a user fails Web authentication, the device maps the MAC address of the user to the Auth-Fail VLAN.

You cannot delete the VLAN that has been configured as an Auth-Fail VLAN. To delete this VLAN, first cancel the Auth-Fail VLAN configuration by using **undo web-auth auth-fail vlan** command.

Examples

Specify VLAN 5 as Web authentication Auth-Fail VLAN on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname–GigabitEthernet1/0/1] port link-type hybrid
```

```
[Sysname–GigabitEthernet1/0/1] mac-vlan enable
[Sysname–GigabitEthernet1/0/1] web-auth auth-fail vlan 5
```

Related commands

display web-auth

web-auth domain

Use **web-auth domain** to specify an authentication domain for Web authentication users on an interface.

Use **undo web-auth domain** to restore the default.

Syntax

web-auth domain *domain-name*

undo web-auth domain

Default

No authentication domain is specified for Web authentication users on an interface.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

domain-name: Specifies an ISP authentication domain name, a case-insensitive string of 1 to 255 characters.

User guidelines

After you configure this command, the device uses the authentication domain for authentication, authorization and accounting (AAA) of the Web authentication users on the interface.

Examples

Specify domain **my-domain** as the authentication domain of Web authentication users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname–GigabitEthernet1/0/1] web-auth domain my-domain
```

web-auth enable

Use **web-auth enable** to enable Web authentication.

Use **undo web-auth enable** to disable Web authentication.

Syntax

web-auth enable apply server *server-name*

undo web-auth enable

Default

Web authentication is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

server-name: Specifies the Web authentication server name, a case-sensitive string of 1 to 32 characters.

User guidelines

Use this command to enable Web authentication on an interface and specify a Web authentication server.

For Web authentication to operate correctly, do not enable port security or configure the port security mode on the Layer 2 Ethernet interface enabled with Web authentication.

Examples

Enable Web authentication and specify Web authentication server **wbs** on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] web-auth enable apply server wbs
```

Related commands

web-auth server

web-auth free-ip

Use **web-auth free-ip** to specify a Web authentication-free subnet.

Use **undo web-auth free-ip** to restore the default.

Syntax

web-auth free-ip *ip-address* { *mask-length* | *mask* }

undo web-auth free-ip { *ip-address* { *mask-length* | *mask* } | **all** }

Default

No Web-authentication-free subnets exist.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the Web authentication-free subnet address.

mask-length: Specifies the mask length of the Web authentication-free subnet address, in the range of 1 to 32.

mask: Specifies a mask for the Web authentication-free subnet in dotted decimal notation.

all: Specifies all Web authentication-free subnets.

User guidelines

Web authentication users can access resources in Web authentication-free subnets without being authenticated.

You can repeat this command to configure multiple Web authentication-free subnets.

Examples

Configure subnet 192.168.0.0/24 as a Web authentication-free subnet.

```
<Sysname> system-view
[Sysname] web-auth free-ip 192.168.0.0 24
```

web-auth max-user

Use **web-auth max-user** to set the maximum number of Web authentication users allowed on an interface.

Use **undo web-auth max-user** to restore the default.

Syntax

web-auth max-user *max-number*

undo web-auth max number

Default

The maximum number of Web authentication users allowed on an interface is 1024.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

max-number: Specifies the maximum number of Web authentication users allowed on an interface. The value range for this argument is 1 to 2048.

User guidelines

If the specified maximum number is smaller than the number of current online Web authentication users on the interface, the limit can be set successfully. The limit does not impact the online Web authentication users. However, the device does not allow new Web authentication users to log in from the interface until the number drops down below the limit.

This command specifies the maximum number of only IPv4 Web authentication users.

Examples

On GigabitEthernet 1/0/1, set the maximum number of Web authentication users to 32.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] web-auth max-user 32
```

Related commands

display web-auth

web-auth offline-detect

Use **web-auth offline-detect** to enable online detection of Web authentication users.

Use **undo web-auth max-user** to disable online detection of Web authentication users.

Syntax

web-auth offline-detect interval *interval*

undo web-auth offline-detect interval

Default

Online detection of Web authentication users is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

interval: Specifies the Web authentication user detection interval, in the range of 60 to 65535 seconds.

User guidelines

This feature enables the device to detect packets of an online user at the specified detection interval. If no packet from the user is received within the interval, the device logs out the user and notifies the RADIUS server to stop accounting for the user.

To prevent the device from mistakenly logging out users, set the detection interval to be the same as the aging time of MAC address entries.

Examples

On GigabitEthernet 1/0/1, enable online detection of Web authentication users and set the detection interval to 3600 seconds.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] web-auth offline-detect interval 3600
```

web-auth proxy port

Use **web-auth proxy port** to add the port number of a Web proxy server, so that HTTP requests forwarded by the Web proxy server trigger Web authentication.

Use **undo web-auth proxy port** to delete one or all Web proxy server port numbers.

Syntax

web-auth proxy port *port number*

undo web-auth proxy port { *port-number* | **all** }

Default

No Web proxy server port numbers are configured on the device.

Views

System view

Predefined user roles

network-admin

Parameters

port number: Specifies a Web proxy server TCP port number, in the range of 1 to 65535.

all: Specifies all Web proxy server TCP port numbers.

User guidelines

By default, proxied HTTP requests cannot trigger Web authentication but are silently dropped. To allow such HTTP requests to trigger Web authentication, specify the port numbers of the Web proxy servers on the device.

You can repeat this command to add the port numbers of multiple Web proxy servers.

If a user's browser uses the Web Proxy Auto-Discovery (WPAD) protocol to discover Web proxy servers, you must perform the following tasks:

- Add the port numbers of the Web proxy servers on the device.
- Configure authentication-free rules to allow user packets destined for the IP address of the WPAD server to pass without authentication.
- For Web authentication to support Web proxy:
- You must add the port numbers of the Web proxy servers on the device.
- Users must make sure their browsers that use a Web proxy server do not use the proxy server for the listening IP address of the local portal Web service. Then, HTTP packets that the Web authentication user sends to the local portal Web service are not sent to the Web proxy server.

Examples

Add the Web proxy server TCP port number of 7777 for Web authentication.

```
<Sysname> system-view
[Sysname] web-auth proxy port 7777
```

web-auth server

Use **web-auth server** to create a Web authentication server and enter its view, or enter the view of an existing Web authentication server.

Use **undo web-auth server** to delete a Web authentication server.

Syntax

web-auth server *server-name*

undo web-auth server *server-name*

Default

No Web authentication servers exist.

Views

System view

Predefined user roles

network-admin

Parameters

server-name: Specifies a Web authentication server name, a case-sensitive string of 1 to 32 characters.

User guidelines

In Web authentication server view, you can configure the following parameters and features for the Web authentication server:

- IP address of the server.
- Redirection URL.

- Parameters to be carried in the redirection URL.

Examples

Create a Web authentication server named **wbs** and enter its view.

```
<Sysname> system-view
[Sysname] web-auth server wbs
[Sysname-web-auth-server-wbs]
```

Related commands

web-auth enable apply server

web-auth timer temp-entry-aging

Use **web-auth timer temp-entry-aging** to configure the aging timer for temporary MAC address entries.

Use **undo web-auth timer temp-entry-aging** to restore the default.

Syntax

web-auth timer temp-entry-aging *aging-time-value*

undo web-auth timer temp-entry-aging

Default

The aging timer for temporary MAC address entries is 60 seconds.

Views

System view

Default command level

network-admin

Parameters

aging-time-value: Specifies the aging timer in seconds for temporary MAC address entries, in the range of 60 to 2147483647.

Usage guidelines

This command is supported only in Release 6343P08 and later.

If Web authentication is enabled, the device generates a temporary MAC address entry when it detects traffic from a user for the first time. The entry records the MAC address, access interface, and VLAN ID of the user, as well as the aging time of the entry.

The aging timer works as follows:

- If the user does not initiate authentication when the aging timer expires, the device deletes the temporary entry.
- If the user passes authentication before the aging timer expires, the device delete the aging timer and records online information for the Web authentication user.
- If the user fails authentication before the aging timer expires and an Auth-Fail VLAN is specified for Web authentication, the device binds the MAC address of the user to the Auth-fail VLAN and reset the aging timer. If the user still fails authentication when the aging timer expires, the device deletes the temporary entry for the user.

As a best practice, change the aging timer to a bigger value in the following cases:

- Web authentication users without access rights frequently send traffic in a short time. As a result, the access device continuously initiates the web authentication process, increasing the load on the device.

- When a user fails authentication, the user does not have enough time to obtain resources from the Auth-Fail VLAN, for example, it failed to download the virus patches.

Examples

Set the aging timer for temporary MAC address entries to 500 seconds.

```
<Sysname> system-view
[Sysname] web-auth timer temp-entry-aging 500
```

Related commands

web-auth auth-fail vlan

Contents

Port security commands

display port-security

Use **display port-security** to display port security configuration, operation information, and statistics for ports.

Syntax

display port-security [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify a port, this command displays port security information for all ports.

Examples

Display port security information for all ports.

```
<Sysname> display port-security
Global port security parameters:
   Port security        : Enabled
   AutoLearn aging time   : 0 min
   Disableport timeout    : 20 s
   Blockmac timeout      : 180 s
   MAC move             : Denied
   Authorization fail    : Online
   NAS-ID profile        : Not configured
   Dot1x-failure trap    : Disabled
   Dot1x-logon trap      : Disabled
   Dot1x-logoff trap     : Enabled
   Intrusion trap        : Disabled
   Address-learned trap   : Enabled
   Mac-auth-failure trap  : Disabled
   Mac-auth-logon trap    : Enabled
   Mac-auth-logoff trap   : Disabled
   Open authentication    : Disabled
   OUI value list        :
    Index :  1         Value : 123401

 GigabitEthernet1/0/1 is link-up
   Port mode                   : userLogin
   NeedToKnow mode              : Disabled
   Intrusion protection mode     : NoAction
   Security MAC address attribute
```

```
   Learning mode           : Sticky
   Aging type              : Periodical
Max secure MAC addresses      : 32
Current secure MAC addresses   : 0
Authorization               : Permitted
NAS-ID profile              : Not configured
Free VLANs                  : Not configured
Open authentication          : Disabled
MAC-move VLAN check bypass    : Disabled
```

Table 1 Command output

Field	Description
Port security	Whether the port security feature is enabled.
AutoLearn aging time	Sticky MAC address aging timer, in minutes or seconds.
Disableport timeout	Silence period (in seconds) of the port that receives illegal packets.
Blockmac timeout	This field is not supported in the current software version. Block timer (in seconds) for MAC addresses in the blocked MAC address list.
MAC move	Status of MAC move: • If the feature is enabled, this field displays **Permitted**. • If the feature is disabled, this field displays **Denied**.
Authorization fail	Action to be taken for users that fail authorization: • **Online**—Allows the users to go online. • **Offline**—Logs off the users.
NAS-ID profile	NAS-ID profile applied globally.
Dot1x-failure trap	Whether SNMP notifications for 802.1X authentication failures are enabled.
Dot1x-logon trap	Whether SNMP notifications for 802.1X authentication successes are enabled.
Dot1x-logoff trap	Whether SNMP notifications for 802.1X authenticated user logoffs are enabled.
Intrusion trap	Whether SNMP notifications for intrusion protection are enabled. If they are enabled, the device sends SNMP notifications after illegal packets are detected.
Address-learned trap	Whether SNMP notifications for MAC address learning are enabled. If they are enabled, the device sends SNMP notifications after it learns a new MAC address.
Mac-auth-failure trap	Whether SNMP notifications for MAC authentication failures are enabled.
Mac-auth-logon trap	Whether SNMP notifications for MAC authentication successes are enabled.
Mac-auth-logoff trap	Whether SNMP notifications for MAC authentication user logoffs are enabled.
Open authentication	Whether global open authentication mode is enabled.
OUI value list	List of OUI values allowed for authentication.

Field	Description
Port mode	Port security mode: • noRestrictions. • autoLearn. • macAddressWithRadius. • macAddressElseUserLoginSecure. • macAddressElseUserLoginSecureExt. • secure. • userLogin. • userLoginSecure. • userLoginSecureExt. • macAddressOrUserLoginSecure. • macAddressOrUserLoginSecureExt. • userLoginWithOUI. For more information about port security modes, see *Security Configuration Guide*.
NeedToKnow mode	Need to know (NTK) mode: • **NeedToKnowOnly**—Forwards only unicast frames with an authenticated destination MAC address. • **NeedToKnowWithBroadcast**—Forwards only broadcast and unicast frames with an authenticated destination MAC address. • **NeedToKnowWithMulticast**—Forwards only broadcast, multicast, and unicast frames with an authenticated destination MAC address. • **NeedToKnowAuto**—Forwards only broadcast, multicast, and unicast frames with an authenticated destination MAC address, and only when the port has online users. • **Disabled**—NTK is disabled.
Intrusion protection mode	Intrusion protection action: • **BlockMacAddress**—Adds the source MAC address of the illegal packet to the blocked MAC address list. • **DisablePort**—Shuts down the port that receives illegal packets permanently. • **DisablePortTemporarily**—Shuts down the port that receives illegal packets for some time. • **NoAction**—Does not perform intrusion protection.
Learning mode	Secure MAC address learning mode: • **Dynamic**. • **Sticky**.
Aging type	Secure MAC address aging type: • **Periodical**—Timer aging only. • **Inactivity**—Inactivity aging feature together with the aging timer.
Max secure MAC addresses	Maximum number of secure MAC addresses (or online users) that port security allows on the port.
Current secure MAC addresses	Number of secure MAC addresses stored.

Field	Description
Authorization	Whether the authorization information from the authentication server (RADIUS server or local device) is ignored: • **Permitted**—Authorization information from the authentication server takes effect. • **Ignored**—Authorization information from the authentication server does not take effect.
NAS-ID profile	NAS-ID profile applied to the port.
Free VLANs	This field is supported only in Release 6328 and later. VLANs in which packets will not trigger authentication. If you do not configure free VLANs, this field displays **Not configured**.
Open authentication	Whether open authentication mode is enabled on the port.
MAC-move VLAN check bypass	Whether the VLAN check bypass feature is enabled for users moving to the port from other ports.

display port-security mac-address block

Use **display port-security mac-address block** to display information about blocked MAC addresses.

Syntax

display port-security mac-address block [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

vlan *vlan-id*: Specifies a VLAN by its ID. The value range is 1 to 4094.

count: Displays only the count of the blocked MAC addresses.

Usage guidelines

If you do not specify any parameters, this command displays information about all blocked MAC addresses.

Examples

Display information about all blocked MAC addresses.

```
<Sysname> display port-security mac-address block
 MAC ADDR           Port                    VLAN ID
 000f-3d80-0d2d     GE1/0/1                 30

 --- On slot 1, 1 MAC address(es) found ---

 --- 1 mac address(es) found ---
```

Display the count of all blocked MAC addresses.

```
<Sysname> display port-security mac-address block count

--- On slot 1, 1 MAC address(es) found ---

--- 1 mac address(es) found ---
```

Table 2 Command output

Field	Description
MAC ADDR	Blocked MAC address.
Port	Port having received frames with the blocked MAC address being the source address.
VLAN ID	ID of the VLAN to which the port belongs.
number mac address(es) found	Number of blocked MAC addresses.

Related commands

port-security intrusion-mode

display port-security mac-address security

Use **display port-security mac-address security** to display information about secure MAC addresses.

Syntax

display port-security mac-address security [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

vlan *vlan-id*: Specifies a VLAN by its ID. The value range is 1 to 4094.

count: Displays only the count of the secure MAC addresses.

Usage guidelines

Secure MAC addresses are those that are automatically learned by the port in autoLearn mode or configured by the **port-security mac-address security** command.

If you do not specify any parameters, this command displays information about all secure MAC addresses.

Examples

Display information about all secure MAC addresses.

```
<Sysname> display port-security mac-address security
 MAC ADDR       VLAN ID  STATE        PORT INDEX               AGING TIME
```

```
0002-0002-0002  1       Secure       GE1/0/1                    Not aged

--- Number of secure MAC addresses: 1 ---
```

Display only the count of the secure MAC addresses.

```
<Sysname> display port-security mac-address security count

--- Number of secure MAC addresses: 1 ---
```

Table 3 Command output

Field	Description
MAC ADDR	Secure MAC address.
VLAN ID	ID of the VLAN to which the port belongs.
STATE	Type of the MAC address. This field displays **Secure** for a secure MAC address.
PORT INDEX	Port to which the secure MAC address belongs.
AGING TIME	The remaining amount of time before the secure MAC address ages out. • If the secure MAC address is a static MAC address, this field displays **Not aged**. • If the secure MAC address is a sticky MAC address, this field displays the remaining lifetime. If the remaining lifetime is less than 60 seconds, the lifetime is counted in seconds. If the lifetime is not less than 60 seconds, the lifetime is counted in minutes. By default, sticky MAC addresses do not age out, and this field displays **Not aged**.
Number of secure MAC addresses	Number of secure MAC addresses stored.

Related commands

port-security mac-address security

port-security access-user log enable

Use **port-security access-user log enable** to enable port security user logging.

Use **undo port-security access-user log enable** to disable port security user logging.

Syntax

port-security access-user log enable [**failed-authorization** | **mac-learning** | **violation** | **vlan-mac-limit**] *

undo port-security access-user log enable [**failed-authorization** | **mac-learning** | **violation** | **vlan-mac-limit**] *

Default

Port security user logging is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

failed-authorization: Logs authorization failures of 802.1X or MAC authentication users.

mac-learning: Logs MAC address learning events.

violation: Logs intrusion protection events.

vlan-mac-limit: Logs the first access attempt from a new MAC access in a VLAN after port security's MAC address limit for that VLAN is reached. For each VLAN, the system does not log any access attempts from new MAC addresses except the first one after the MAC address limit is reached.

Usage guidelines

To prevent excessive port security user log entries, use this feature only if you need to analyze abnormal port security user events.

If you do not specify any parameters, this command enables all types of port security user logs.

Examples

Enable intrusion protection event logging.

```
<Sysname> system-view
[Sysname] port-security access-user log enable violation
```

Related commands

info-center source portsec logfile deny (*Network Management and Monitoring Command Reference*)

port-security authentication open

Use **port-security authentication open** to enable open authentication mode on a port.

Use **undo port-security authentication open** to disable open authentication mode on a port.

Syntax

port-security authentication open

undo port-security authentication open

Default

Open authentication mode is disabled on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

This command enables access users (802.1X or MAC authentication users) of a port to come online and access the network even if they use nonexistent usernames or incorrect passwords.

Access users that come online in open authentication mode are called open users. Authorization and accounting are not available for open users. To display open user information, use the following commands:

- **display dot1x connection open**.
- **display mac-authentication connection open**.

Open authentication mode does not affect the access of users that use correct user information on the port.

The open authentication mode setting has lower priority than the 802.1X Auth-Fail VLAN and the MAC authentication guest VLAN. Open authentication mode does not take effect on a port if the port is also configured with the 802.1X Auth-Fail VLAN or the MAC authentication guest VLAN.

For information about 802.1X authentication or MAC authentication, see *Security Configuration Guide*.

Examples

Enable open authentication mode on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security authentication open
```

Related commands

display dot1x connection

display mac-authentication connection

port-security authentication open global

port-security authentication open global

Use **port-security authentication open global** to enable global open authentication mode.

Use **undo port-security authentication open global** to disable global open authentication mode.

Syntax

port-security authentication open global

undo port-security authentication open global

Default

Global open authentication mode is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command enables access users (802.1X or MAC authentication users) to come online and access the network even if they use nonexistent usernames or incorrect passwords.

Access users that come online in open authentication mode are called open users. Authorization and accounting are not available for open users. To display open user information, use the following commands:

- **display dot1x connection open**.
- **display mac-authentication connection open**.

Open authentication mode does not affect the access of users that use correct user information.

The open authentication mode setting has lower priority than the 802.1X Auth-Fail VLAN and the MAC authentication guest VLAN. Open authentication mode does not take effect on a port if the port is also configured with the 802.1X Auth-Fail VLAN or the MAC authentication guest VLAN.

For information about 802.1X authentication or MAC authentication, see *Security Configuration Guide*.

Examples

Enable global open authentication mode.

```
<Sysname> system-view
[Sysname] port-security authentication open global
```

Related commands

display dot1x connection

display mac-authentication connection

port-security authentication open

port-security authorization ignore

Use **port-security authorization ignore** to configure a port to ignore the authorization information received from the authentication server (a RADIUS server or the local device).

Use **undo port-security authorization ignore** to restore the default.

Syntax

port-security authorization ignore

undo port-security authorization ignore

Default

A port uses the authorization information from the server.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

After a user passes RADIUS or local authentication, the server performs authorization based on the authorization attributes configured for the user account. For example, the server can assign a VLAN. If you do not want the port to use such authorization attributes for users, use this command to ignore the authorization information from the server.

Examples

Configure GigabitEthernet 1/0/1 to ignore the authorization information from the authentication server.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security authorization ignore
```

Related commands

display port-security

port-security authorization-fail offline

Use **port-security authorization-fail offline** to enable the authorization-fail-offline feature.

Use **undo port-security authorization-fail offline** to disable the authorization-fail-offline feature.

Syntax

port-security authorization-fail offline [**quiet-period**]

undo port-security authorization-fail offline

Default

The authorization-fail-offline feature is disabled. The device does not log off users that have failed authorization.

Views

System view

Predefined user roles

network-admin

Parameters

quiet-period: Enables the quiet timer for 802.1X or MAC authentication users that are logged off by the authorization-fail-offline feature. The device adds these users to the 802.1X or MAC authentication quiet queue. Within the quiet timer, the device does not process packets from these users or authenticate them. If you do not specify this keyword, the quiet timer feature is disabled for users that are logged off by the authorization-fail-offline feature. The device immediately authenticates these users upon receiving packets from them.

Usage guidelines

The authorization-fail-offline feature logs off port security users that have failed ACL or user profile authorization.

A user fails ACL or user profile authorization in the following situations:

- The device or server fails to assign the specified ACL or user profile to the user.
- The device or server assigns an ACL or user profile that does not exist on the device to the user.

If this feature is disabled, the device does not log off users that have failed ACL or user profile authorization. However, the device outputs messages to report the failure.

For the **quiet-period** keyword to take effect, complete the following tasks:

- For 802.1X users, use the **dot1x quiet-period** command to enable the quiet timer and use the **dot1x timer quiet-period** command to set the timer.
- For MAC authentication users, use the **mac-authentication timer quiet** command to set the quiet timer for MAC authentication.

Examples

Enable the authorization-fail-offline feature.

```
<Sysname> system-view
[Sysname] port-security authorization-fail offline
```

Related commands

display port-security

dot1x quiet-period

dot1x timer quiet-period

mac-authentication timer

port-security enable

Use **port-security enable** to enable port security.

Use **undo port-security enable** to disable port security.

Syntax

port-security enable

undo port-security enable

Default

Port security is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

You must disable global 802.1X and MAC authentication before you enable port security on a port.

Enabling or disabling port security resets the following security settings to the default:

- 802.1X access control mode is MAC-based.
- Port authorization state is auto.

When online users are present on a port, disabling port security logs off the online users.

Examples

Enable port security.

```
<Sysname> system-view
[Sysname] port-security enable
```

Related commands

display port-security

dot1x

dot1x port-control

dot1x port-method

mac-authentication

port-security free-vlan

Use **port-security free-vlan** to configure free VLANs for port security.

Use **undo port-security free-vlan** to restore the default.

Syntax

port-security free-vlan *vlan-id-list*

undo port-security free-vlan *vlan-id-list*

Default

No free VLANs are configured for port security on a port. Authentication will be triggered by packets from users in any VLAN on the port that is configured with 802.1X, MAC authentication, or a port security authentication mode.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 VLAN items. Each VLAN item specifies a VLAN by VLAN ID or specifies a range of VLANs in the form of *start-vlan-id* to *end-vlan-id*. The value range for VLAN IDs is 1 to 4094. The end VLAN ID must be equal to or greater than the start VLAN ID.

Usage guidelines

This command is supported only in Release 6328 and later.

This command allows packets from the specified VLANs to not trigger 802.1X or MAC authentication on a port configured with any of the following features:

- 802.1X authentication.
- MAC authentication.
- Any of the following port security modes:
  - userLogin.
  - userLoginSecure.
  - userLoginWithOUI.
  - userLoginSecureExt.
  - macAddressWithRadius.
  - macAddressOrUserLoginSecure.
  - macAddressElseUserLoginSecure.
  - macAddressOrUserLoginSecureExt.
  - macAddressElseUserLoginSecureExt.

Execute this command multiple times to specify multiple free VLANs for port security.

Examples

Configure free VLANs for port security on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security free-vlan 2 3
```

Related commands

display port-security

port-security intrusion-mode

Use **port-security intrusion-mode** to configure the intrusion protection action to take when intrusion protection detects illegal frames on a port.

Use **undo port-security intrusion-mode** to restore the default.

Syntax

port-security intrusion-mode { blockmac | disableport | disableport-temporarily }

undo port-security intrusion-mode

Default

Intrusion protection is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

blockmac: Adds the source MAC addresses of illegal frames to the blocked MAC address list and discards frames with blocked source MAC addresses for a period set by the block timer. A blocked MAC address will be unblocked when the block timer expires. The timer is fixed at 3 minutes. To display the blocked MAC address list, use the **display port-security mac-address block** command.

disableport: Disables the port permanently when an illegal frame is received on the port.

disableport-temporarily: Disables the port for a period of time whenever it receives an illegal frame. You can use the **port-security timer disableport** command to set the period.

Usage guidelines

To bring up the port disabled by the intrusion protection feature, use the **undo shutdown** command.

Examples

Configure GigabitEthernet 1/0/1 to block the source MAC addresses of illegal frames after intrusion protection detects the illegal frames.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security intrusion-mode blockmac
```

Related commands

display port-security

display port-security mac-address block

port-security timer disableport

port-security mac-address aging-type inactivity

Use **port-security mac-address aging-type inactivity** to enable inactivity aging for secure MAC addresses.

Use **undo port-security mac-address aging-type inactivity** to disable inactivity aging for secure MAC addresses.

Syntax

port-security mac-address aging-type inactivity

undo port-security mac-address aging-type inactivity

Default

The inactivity aging feature is disabled for secure MAC addresses.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

This command enables the device to periodically detect traffic data from secure MAC addresses.

If only the aging timer is configured, the aging timer counts up regardless of whether traffic data has been sent from the secure MAC addresses. When you use the aging timer together with the inactivity aging feature, the aging timer restarts once traffic data is detected from the secure MAC addresses. The secure MAC addresses age out only when no traffic data is detected within the aging timer.

The inactivity aging feature prevents the unauthorized use of a secure MAC address when the authorized user is offline. The feature also removes outdated secure MAC addresses so that new secure MAC addresses can be learned or configured.

If the aging timer is set to a value not less than 60 seconds, the traffic data detection interval is fixed at 30 seconds.

If the aging timer is set to a value less than 60 seconds, the traffic data detection interval is the effective aging period.

To set the aging timer for secure MAC addresses, use the **port-security timer autolearn aging** command.

This command takes effect only on sticky MAC addresses and dynamic secure MAC addresses.

Examples

Enable inactivity aging for secure MAC addresses on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security mac-address aging-type inactivity
```

Related commands

display port-security

port-security mac-address dynamic

Use **port-security mac-address dynamic** to enable the dynamic secure MAC feature.

Use **undo port-security mac-address dynamic** to disable the dynamic secure MAC feature.

Syntax

port-security mac-address dynamic

undo port-security mac-address dynamic

Default

The dynamic secure MAC feature is disabled. Sticky MAC addresses can be saved to the configuration file. Once saved, they survive a device reboot.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

The dynamic secure MAC feature converts sticky MAC addresses to dynamic and disables saving them to the configuration file.

After you execute this command, you cannot manually configure sticky MAC addresses, and secure MAC addresses learned by a port in autoLearn mode are dynamic. All dynamic MAC addresses are lost at reboot. Use this command when you want to clear all sticky MAC addresses after a device reboot.

You can display dynamic secure MAC addresses by using the **display port-security mac-address security** command.

The **undo port-security mac-address dynamic** command converts all dynamic secure MAC addresses on the port to sticky MAC addresses. You can manually configure sticky MAC addresses.

Examples

Enable the dynamic secure MAC feature on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security mac-address dynamic
```

Related commands

display port-security

display port-security mac-address security

port-security mac-address security

Use **port-security mac-address security** to add a secure MAC address.

Use **undo port-security mac-address security** to remove a secure MAC address.

Syntax

In Layer 2 Ethernet interface view:

port-security mac-address security [**sticky**] *mac-address* **vlan** *vlan-id*

undo port-security mac-address security [**sticky**] *mac-address* **vlan** *vlan-id*

In system view:

port-security mac-address security [**sticky**] *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*

undo port-security mac-address security [[*mac-address* [**interface** *interface-type interface-number*]] **vlan** *vlan-id*]

Default

No manually configured secure MAC address entries exist.

Views

System view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

sticky: Specifies the MAC address type as sticky. If you do not specify this keyword, the command configures a static secure MAC address.

mac-address: Specifies a MAC address, in H-H-H format.

interface *interface-type interface-number*: Specifies a port by its type and number.

vlan *vlan-id*: Specifies the VLAN to which the secure MAC address belongs. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

Secure MAC addresses are MAC addresses configured or learned in autoLearn mode, and if saved, can survive a device reboot. You can bind a secure MAC address only to one port in a VLAN.

You can add important or frequently used MAC addresses as sticky or static secure MAC addresses to avoid the secure MAC address limit causing authentication failure. To successfully add secure MAC addresses on a port, first complete the following tasks:

- Enable port security on the port.
- Set the port security mode to autoLearn.
- Configure the port to permit packets of the specified VLAN to pass or add the port to the VLAN. Make sure the VLAN already exists.

Sticky MAC addresses can be manually configured or automatically learned in autoLearn mode. Sticky MAC addresses do not age out by default. You can use the **port-security timer autolearn aging** command to set an aging timer for the sticky MAC addresses. When the timer expires, the sticky MAC addresses are removed.

Static secure MAC addresses never age out unless you perform the following operations:

- Remove these MAC addresses by using the **undo port-security mac-address security** command.
- Change the port security mode.
- Disable the port security feature.

You cannot change the type of a secure address entry that has been added or add two entries that are identical except for their entry type. For example, you cannot add the **port-security mac-address security sticky 1-1-1 vlan 10** entry when a **port-security mac-address security 1-1-1 vlan 10** entry exists. To add the new entry, you must delete the old entry.

Examples

Enable port security, set GigabitEthernet 1/0/1 to operate in autoLearn mode, and configure the port to support a maximum number of 100 secure MAC addresses.

```
<Sysname> system-view
[Sysname] port-security enable
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security max-mac-count 100
[Sysname-GigabitEthernet1/0/1] port-security port-mode autolearn
```

Specify MAC address 0001-0002-0003 in VLAN 4 as a sticky MAC address.

```
[Sysname-GigabitEthernet1/0/1] port-security mac-address security sticky 0001-0002-0003
vlan 4
[Sysname-GigabitEthernet1/0/1] quit
```

In system view, specify MAC address 0001-0001-0002 in VLAN 10 as a secure MAC address for GigabitEthernet 1/0/1.

```
[Sysname] port-security mac-address security 0001-0001-0002 interface gigabitethernet
1/0/1 vlan 10
```

Related commands

display port-security

port-security timer autolearn aging

port-security mac-limit

Use **port-security mac-limit** to set the maximum number of MAC addresses that port security allows for specific VLANs on a port.

Use **undo port-security mac-limit** to restore the default.

Syntax

port-security mac-limit *max-number* **per-vlan** *vlan-id-list*

undo port-security mac-limit *max-number* **per-vlan** *vlan-id-list*

Default

The maximum number is 2147483647.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

max-number: Specifies the maximum number of MAC addresses. The value range is 1 to 2147483647.

per-vlan *vlan-id-list*: Applies the maximum number to a VLAN list on per-VLAN basis. The *vlan-id-list* argument specifies a space-separated list of up to 10 VLAN items. Each VLAN item specifies a VLAN by VLAN ID or specifies a range of VLANs in the form of *vlan-id1* **to** *vlan-id2*. The value range for the VLAN IDs is 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument.

Usage guidelines

This command limits the number of MAC addresses that port security allows to access a port through specific VLANs. Use this command to prevent resource contentions among MAC addresses and ensure reliable performance for each access user on the port. When the number of MAC addresses in a VLAN on the port reaches the upper limit, the device denies any subsequent MAC addresses in the VLAN on the port.

Port security allows the access of the following types of MAC addresses on a port:

- MAC addresses that pass 802.1X or MAC authentication.
- MAC addresses in the MAC authentication guest VLAN or MAC authentication critical VLAN.
- MAC addresses in the 802.1X guest VLAN, 802.1X Auth-Fail VLAN, or 802.1X critical VLAN.

On a port, the maximum number of MAC addresses in a VLAN cannot be smaller than the number of existing MAC addresses in the VLAN. If the specified maximum number is smaller, the setting does not take effect.

Examples

On GigabitEthernet 1/0/1, configure VLAN 1, VLAN 5, and VLANs 10 through 20 each to allow a maximum of 32 MAC authentication and 802.1X users.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security mac-limit 32 per-vlan 1 5 10 to 20
```

Related commands

display dot1x

display mac-authentication

port-security mac-move bypass-vlan-check

Use **port-security mac-move bypass-vlan-check** to enable VLAN check bypass on a port for users moving to it.

Use **undo port-security mac-move bypass-vlan-check** to disable VLAN check bypass on a port for users moving to it.

Syntax

port-security mac-move bypass-vlan-check

undo port-security mac-move bypass-vlan-check

Default

VLAN check bypass is disabled in port security for users moving to a port. When reauthenticating a user that has moved to the port, the device examines whether the VLAN to which the user belongs is permitted by the port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

This command is supported only in Release 6318P01 and later.

Enable VLAN check bypass on a port to skip checking VLAN information in the packets that trigger 802.1X authentication or MAC authentication for users moving to that port.

For a user moving between ports, the port from which the user moves is called the source port and the port to which the user moves is called the destination port.

When you configure VLAN check bypass, follow these guidelines:

- To ensure a successful reauthentication, enable VLAN check bypass on a destination port if the source port is enabled with MAC-based VLAN.
- If the destination port is an 802.1X-enabled trunk port, you must configure it to send 802.1X protocol packets without VLAN tags.

Examples

Enable VLAN check bypass for users moving to GigabitEthernet 1/0/1 from other ports.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security mac-move bypass-vlan-check
```

Related commands

display port-security

dot1x eapol untag

port-security mac-move permit

port-security mac-move permit

Use **port-security mac-move permit** to enable MAC move on the device.

Use **undo port-security mac-move permit** to disable MAC move on the device.

Syntax

port-security mac-move permit

undo port-security mac-move permit

Default

MAC move is disabled on the device.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Port security MAC move takes effect in the following scenarios:

- **Inter-port move on a device**—An online user authenticated through 802.1X or MAC authentication moves between ports on the device. The user VLAN or authentication method might change or stay unchanged after the move.
- **Inter-VLAN move on a port**—An online user authenticated through 802.1X or MAC authentication moves between VLANs on a trunk or hybrid port. In addition, the packets that trigger authentication have VLAN tags.

Port security MAC move allows an online user authenticated through 802.1X or MAC authentication on one port or VLAN to be reauthenticated and come online on another port or VLAN without going offline first. After the user passes authentication on the new port or VLAN, the system removes the authentication session of the user on the original port or VLAN.

NOTE:

For MAC authentication, the MAC move feature applies only when MAC authentication single-VLAN mode is used. The MAC move feature does not apply to MAC authentication users that move between VLANs on a port with MAC authentication multi-VLAN mode enabled.

If this feature is disabled, 802.1X or MAC authenticated users must go offline first before they can be reauthenticated successfully on a new port or VLAN to come online.

802.1X or MAC authenticated users cannot move between ports on a device or between VLANs on a port if the maximum number of online users on the authentication server has been reached.

Examples

Enable MAC move.

```
<Sysname> system-view
[Sysname] port-security mac-move permit
```

Related commands

display port-security

mac-authentication host-mode multi-vlan

port-security max-mac-count

Use **port-security max-mac-count** to set the maximum number of secure MAC addresses that port security allows on a port.

Use **undo port-security max-mac-count** to restore the default.

Syntax

port-security max-mac-count *max-count* [**vlan** [*vlan-id-list*]]

undo port-security max-mac-count [**vlan** [*vlan-id-list*]]

Default

Port security does not limit the number of secure MAC addresses on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

max-count: Specifies the maximum number of secure MAC addresses that port security allows on the port. The value range is 1 to 2147483647.

vlan [*vlan-id-list*]: Specifies a space-separated list of up to 10 VLAN items. Each VLAN item specifies a VLAN ID or a range of VLAN IDs in the form of *start-vlan-id* **to** *end-vlan-id*. The end VLAN ID cannot be smaller than the start VLAN ID. The value range for VLAN IDs is 1 to 4094. If you do not specify the **vlan** keyword, this command sets the maximum number of secure MAC addresses that port security allows on a port. If you do not specify the *vlan-id-list* argument, this command sets the maximum number of secure MAC addresses for each VLAN on the port. This option takes effect only on a port that operates in autoLearn mode.

Usage guidelines

For autoLearn mode, this command sets the maximum number of secure MAC addresses (both configured and automatically learned) on the port.

In any other mode that enables 802.1X, MAC authentication, or both, this command sets the maximum number of authenticated MAC addresses on the port. The actual maximum number of concurrent users that the port accepts equals the smaller of the following values:

- The value set by using this command.
- The maximum number of concurrent users allowed by the authentication mode in use.

For example, in userLoginSecureExt mode, if 802.1X allows more concurrent users than port security's limit on the number of MAC addresses, port security's limit takes effect.

When you configure this command, follow these guidelines and restrictions:

- Make sure the maximum number of secure MAC addresses for a VLAN is not less than the number of MAC addresses currently saved for the VLAN.
- If you execute this command multiple times to set the maximum number of secure MAC addresses for the same VLAN, the most recent configuration takes effect.

- You cannot change port security's limit on the number of MAC addresses when the port is operating in autoLearn mode.

Examples

Set the maximum number of secure MAC address port security allows on GigabitEthernet 1/0/1 to 100.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security max-mac-count 100
```

Related commands

display port-security

port-security nas-id-profile

Use **port-security nas-id-profile** to apply a NAS-ID profile to global or port-based port security.

Use **undo port-security nas-id-profile** to restore the default.

Syntax

port-security nas-id-profile *profile-name*

undo port-security nas-id-profile

Default

No NAS-ID profile is applied to port security globally or on any port.

Views

System view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

profile-name: Specifies a NAS-ID profile by its name. The argument is a case-insensitive string of 1 to 31 characters.

Usage guidelines

A NAS-ID profile defines NAS-ID and VLAN bindings. You can create a NAS-ID profile by using the **aaa nas-id profile** command.

The device selects a NAS-ID profile for a port in the following order:

1. The port-specific NAS-ID profile.
2. The NAS-ID profile applied globally.

If no NAS-ID profile is applied or no matching binding is found in the selected profile, the device uses the device name as the NAS-ID.

Examples

Apply NAS-ID profile **aaa** to GigabitEthernet 1/0/1 for port security.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security nas-id-profile aaa
```

Globally apply NAS-ID profile **aaa** to port security.

```
<Sysname> system-view
[Sysname] port-security nas-id-profile aaa
```

Related commands

aaa nas-id profile

port-security ntk-mode

Use **port-security ntk-mode** to configure the NTK feature.

Use **undo port-security ntk-mode** to restore the default.

Syntax

port-security ntk-mode { **ntk-withbroadcasts** | **ntk-withmulticasts** | **ntkauto** | **ntkonly** }

undo port-security ntk-mode

Default

The NTK feature is not configured on a port and all frames are allowed to be sent.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

ntk-withbroadcasts: Forwards only broadcast and unicast frames with an authenticated destination MAC address.

ntk-withmulticasts: Forwards only broadcast, multicast, and unicast frames with an authenticated destination MAC address.

ntkauto: Forwards only broadcast, multicast, and unicast frames with an authenticated destination MAC address, and only when the port has online users.

ntkonly: Forwards only unicast frames with an authenticated destination MAC address.

Usage guidelines

The NTK feature checks the destination MAC addresses in outbound frames. This feature allows frames to be sent only to devices passing authentication, preventing illegal devices from intercepting network traffic.

Examples

Set the NTK mode of GigabitEthernet 1/0/1 to **ntkonly**, allowing the port to forward received packets only to devices passing authentication.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security ntk-mode ntkonly
```

Related commands

display port-security

port-security oui

Use **port-security oui** to configure an OUI value for user authentication.

Use **undo port-security oui** to delete the OUI value with the specified OUI index.

Syntax

port-security oui index *index-value* **mac-address** *oui-value*

undo port-security oui index *index-value*

Default

No OUI values are configured.

Views

System view

Predefined user roles

network-admin

Parameters

index-value: Specifies the OUI index, in the range of 1 to 16.

oui-value: Specifies an OUI string, a 48-bit MAC address in the H-H-H format. The system uses only the 24 high-order bits as the OUI value.

Usage guidelines

You can configure multiple OUI values.

An OUI, the first 24 binary bits of a MAC address, is assigned by IEEE to uniquely identify a device vendor. Use this command to allow devices of specific vendors to access the network without being authenticated. For example, you can specify the OUIs of IP phones and printers.

The OUI values configured by this command apply only to the ports operating in userLoginWithOUI mode. In userLoginWithOUI mode, a port allows only one 802.1X user and one user whose MAC address matches one of the configured OUI values.

Examples

Configure an OUI value of 000d2a, and set the index to 4.

```
<Sysname> system-view
[Sysname] port-security oui index 4 mac-address 000d-2a10-0033
```

Related commands

display port-security

port-security packet-detect arp-source-ip factor

Use **port-security packet-detect arp-source-ip factor** to specify an IP address and mask for calculating the source IP of ARP detection packets.

Use **undo port-security packet-detect arp-source-ip factor** to restore the default.

NOTE:

This command is supported only in Release 6348P01 and later.

Syntax

port-security packet-detect arp-source-ip factor *ip-address* { *mask* | *mask-length* }

undo port-security packet-detect arp-source-ip factor

Default

No IP address or mask is specified for calculating the source IP of ARP detection packets. The source IP of ARP detection packets is 0.0.0.0.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address { *mask* | *mask-length* }: Specifies an IP address and mask for calculating the source IP of ARP detection packets. The *mask* argument represents the IP address mask, in dotted decimal notation. The mask cannot be 255.255.255.255. The *mask-length* argument represents the IP address mask length, in the range of 0 to 31.

Usage guidelines

By default, the device uses 0.0.0.0 as the source IP address of ARP detection packets. The network might have users that cannot respond to ARP detection packets with source IP address 0.0.0.0. As a result, the device inadequately determines that these users have gone offline. To resolve the issue, use this command to specify an IP address and mask for calculating the source IP of ARP detection packets sent to a user in conjunction with the user's IP address.

The device uses the following formula to calculate the source IP address of ARP detection packets: source IP = (user IP & specified mask) | (specified IP & ~specified mask). The ~mask parameter represents the reverse of a mask. For example, the reverse mask of 255.255.255.0 is 0.0.0.255. If the IP address of a user is 192.168.8.1/24 and the IP address and mask specified by using this command is 1.1.1.11/255.255.255.0, the source IP address of ARP detection packets is 192.168.8.11/24.

To avoid the source IP address of ARP detection packets being the same as the destination IP address, follow these restrictions and guidelines:

- The mask length specified by using this command must be equal to or longer than the mask length of users' IP addresses.
- The mask cannot be 255.255.255.255.

This command takes effect only on users that come online after this command is executed.

Examples

Specify 0.0.0.11/24 for calculating the source IP of ARP detection packets.

```
<Sysname> system-view
[Sysname] port-security packet-detect arp-source-ip factor 0.0.0.11 24
```

Related commands

mac-authentication packet-detect retry

dot1x packet-detect retry

port-security port-mode

Use **port-security port-mode** to set the port security mode of a port.

Use **undo port-security port-mode** to restore the default.

Syntax

port-security port-mode { autolearn | mac-authentication | mac-else-userlogin-secure | mac-else-userlogin-secure-ext | secure |

userlogin | userlogin-secure | userlogin-secure-ext | userlogin-secure-or-mac | userlogin-secure-or-mac-ext | userlogin-withoui }

undo port-security port-mode

Default

A port operates in noRestrictions mode, where port security does not take effect.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

Keyword	Security mode	Description
autolearn	autoLearn	A port in this mode can learn MAC addresses. The automatically learned MAC addresses are not added to the MAC address table as dynamic MAC address. Instead, the MAC addresses are added to the secure MAC address table as secure MAC addresses. You can also configure secure MAC addresses by using the **port-security mac-address security** command. A port in autoLearn mode allows frames sourced from the following MAC addresses to pass: • Secure MAC addresses. • MAC addresses configured by using the **mac-address dynamic** and **mac-address static** commands. When the number of secure MAC addresses reaches the upper limit set by the **port-security max-mac-count** command, the port changes to **secure** mode.
mac-authentication	macAddressWithRadius	In this mode, a port performs MAC authentication for users and services multiple users.
mac-else-userlogin-secure	macAddressElseUserLoginSecure	This mode is the combination of the macAddressWithRadius and userLoginSecure modes, with MAC authentication having a higher priority. In this mode, the port allows one 802.1X authentication user and multiple MAC authentication users to log in. • Upon receiving a non-802.1X frame, a port in this mode performs only MAC authentication. • Upon receiving an 802.1X frame, the port performs MAC authentication and then, if MAC authentication fails, 802.1X authentication.
mac-else-userlogin-secure-ext	macAddressElseUserLoginSecureExt	Same as the macAddressElseUserLoginSecure mode except that a port in this mode supports multiple 802.1X and MAC authentication users.

Keyword	Security mode	Description
secure	secure	In this mode, MAC address learning is disabled on the port and you can configure MAC addresses by using the **mac-address static** and **mac-address dynamic** commands. The port permits only frames sourced from the following MAC addresses to pass: • Secure MAC addresses. • MAC addresses configured by using the **mac-address static** and **mac-address dynamic** commands.
userlogin	userLogin	In this mode, a port performs 802.1X authentication and implements port-based access control. If one 802.1X user passes authentication, all the other 802.1X users of the port can access the network without authentication.
userlogin-secure	userLoginSecure	In this mode, a port performs 802.1X authentication and implements MAC-based access control. The port services only one user passing 802.1X authentication.
userlogin-secure-ext	userLoginSecureExt	Same as the userLoginSecure mode, except that this mode supports multiple online 802.1X users.
userlogin-secure-or-mac	macAddressOrUserLoginSecure	This mode is the combination of the userLoginSecure and macAddressWithRadius modes. In this mode, the port allows one 802.1X authentication user and multiple MAC authentication users to log in. In this mode, the port performs 802.1X authentication first. By default, if 802.1X authentication fails, MAC authentication is performed. However, the port in this mode processes authentication differently when the following conditions exist: • The port is enabled with parallel processing of MAC authentication and 802.1X authentication. • The port is enabled with the 802.1X unicast trigger. • The port receives a packet from an unknown MAC address. Under such conditions, the port sends a unicast EAP-Request/Identity packet to the MAC address to initiate 802.1X authentication. After that, the port immediately processes MAC authentication without waiting for the 802.1X authentication result.
userlogin-secure-or-mac-ext	macAddressOrUserLoginSecureExt	Same as the macAddressOrUserLoginSecure mode, except that a port in this mode supports multiple 802.1X and MAC authentication users.
userlogin-withoui	userLoginWithOUI	Similar to the userLoginSecure mode. In addition, a port in this mode also permits frames from a user whose MAC address contains a specific OUI. In this mode, the port performs OUI check at first. If the OUI check fails, the port performs 802.1X authentication. The port permits frames that pass OUI check or 802.1X authentication.

Usage guidelines

To change the security mode for a port security enabled port, you must set the port in noRestrictions mode first. Do not change port security mode when the port has online users.

IMPORTANT:

If you are configuring the autoLearn mode, first set port security's limit on the number of secure MAC addresses by using the **port-security max-mac-count** command. You cannot change the setting when the port is operating in autoLearn mode.

When port security is enabled, you cannot enable 802.1X or MAC authentication, or change the access control mode or port authorization state. The port security automatically modifies these settings in different security modes.

As a best practice, do not enable the **mac-else-userlogin-secure** or **mac-else-userlogin-secure-ext** mode on the port where MAC authentication delay is enabled. The two modes are mutually exclusive with the MAC authentication delay feature. For more information about MAC authentication delay, see "MAC authentication commands."

Examples

Enable port security, and set GigabitEthernet 1/0/1 to operate in secure mode.

```
<Sysname> system-view
[Sysname] port-security enable
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security port-mode secure
```

Change the port security mode of GigabitEthernet 1/0/1 to userLogin.

```
[Sysname-GigabitEthernet1/0/1] undo port-security port-mode
[Sysname-GigabitEthernet1/0/1] port-security port-mode userlogin
```

Related commands

display port-security

port-security max-mac-count

port-security timer autolearn aging

Use **port-security timer autolearn aging** to set the secure MAC aging timer.

Use **undo port-security timer autolearn aging** to restore the default.

Syntax

port-security timer autolearn aging [**second**] *time-value*

undo port-security timer autolearn aging

Default

Secure MAC addresses do not age out.

Views

System view

Predefined user roles

network-admin

Parameters

second: Specifies the aging timer in seconds for secure MAC addresses. If you do not specify this keyword, the command sets the aging timer in minutes for secure MAC addresses.

time-value: Specifies the aging timer. The value range is 0 to 129600 if the unit is minute. To disable the aging timer, set the timer to 0. The value range is 10 to 7776000 if the unit is second.

Usage guidelines

The timer applies to all sticky secure MAC addresses and those automatically learned by a port.

The effective aging timer varies by the aging timer setting:

- If the aging timer is set in seconds, the effective aging timer can be either of the following values:
  - The nearest multiple of 30 seconds to the configured aging timer if the configured timer is not less than 60 seconds. The effective aging timer is not less than the configured aging timer.
  - The configured aging timer if the configured timer is less than 60 seconds.
- If the aging timer is set in minutes, the effective aging timer is the configured aging timer.

A short aging time improves port access security and port resource utility but affects online user stability. Set an appropriate secure MAC address aging timer according to your device performance and the network environment.

When a short aging time (less than 60 seconds) works with inactivity aging, do not assign a large value to the maximum number of secure MAC addresses on a port. A large value in this case might affect device performance.

Examples

Set the secure MAC aging timer to 30 minutes.

```
<Sysname> system-view
[Sysname] port-security timer autolearn aging 30
```

Set the secure MAC aging timer to 50 seconds.

```
<Sysname> system-view
[Sysname] port-security timer autolearn aging second 50
```

Related commands

display port-security

port-security mac-address security

port-security timer disableport

Use **port-security timer disableport** to set the silence period during which the port remains disabled.

Use **undo port-security timer disableport** to restore the default.

Syntax

port-security timer disableport *time-value*

undo port-security timer disableport

Default

The port silence period is 20 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

time-value: Specifies the silence period in seconds during which the port remains disabled. The value is in the range of 20 to 300.

Usage guidelines

If you configure the intrusion protection action as disabling the port temporarily, use this command to set the silence period.

Examples

Configure the intrusion protection action on GigabitEthernet 1/0/1 as disabling the port temporarily, and set the port silence period to 30 seconds.

```
<Sysname> system-view
[Sysname] port-security timer disableport 30
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security intrusion-mode disableport-temporarily
```

Related commands

display port-security

port-security intrusion-mode

port-security traffic-statistics enable

Use **port-security traffic-statistics enable** to enable traffic statistics for 802.1X and MAC authentication users.

Use **undo port-security traffic-statistics enable** to disable traffic statistics for 802.1X and MAC authentication users.

Syntax

port-security traffic-statistics enable

undo port-security traffic-statistics enable

Default

The device does not collect traffic statistics for 802.1X and MAC authentication users. 802.1X and MAC authentication user statistics collected and sent to the accounting server only include the online duration of the users.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command is available in Release 6312 and later.

To collect and send traffic statistics of 802.1X and MAC authentication users to the accounting server in addition to their online duration, use this command to enable the traffic statistics feature for 802.1X and MAC authentication users.

This feature takes effect only on users that come online after the feature is enabled.

This feature takes effect on 802.1X and MAC authentication users when port security is enabled, or when 802.1X and MAC authentication are separately enabled on the device.

If a port performs MAC authentication or 802.1X authentication in MAC-based access control mode, this feature collects user traffic statistics on a per-MAC basis on the port.

If a port performs 802.1X authentication in port-based access control mode, this feature collects user traffic statistics on a per-port basis on the port.

With this feature enabled, the device requires more ACL resources for new 802.1X or MAC authentication users. If the device has run out of ACL resources, the authentication will fail for new 802.1X or MAC authentication users.

Enable this feature only if traffic accounting is required and only if there are sufficient ACL resources. If the network has a large number of online 802.1X and MAC authentication users when this feature is enabled, ACL resources might become insufficient. This issue causes authentication failure of new 802.1X and MAC authentication users. For more information about 802.1X and MAC authentication, see *Security Configuration Guide*.

Examples

Enable traffic statistics for 802.1X and MAC authentication users.

```
<Sysname> system-view
[Sysname] port-security traffic-statistics enable
```

snmp-agent trap enable port-security

Use **snmp-agent trap enable port-security** to enable SNMP notifications for port security.

Use **undo snmp-agent trap enable port-security** to disable SNMP notifications for port security.

Syntax

snmp-agent trap enable port-security [**address-learned** | **dot1x-failure** | **dot1x-logoff** | **dot1x-logon** | **intrusion** | **mac-auth-failure** | **mac-auth-logoff** | **mac-auth-logon**] *

undo snmp-agent trap enable port-security [**address-learned** | **dot1x-failure** | **dot1x-logoff** | **dot1x-logon** | **intrusion** | **mac-auth-failure** | **mac-auth-logoff** | **mac-auth-logon**] *

Default

All port security SNMP notifications are disabled.

Views

System view

Predefined user roles

network-admin

Parameters

address-learned: Specifies notifications about MAC address learning.

dot1x-failure: Specifies notifications about 802.1X authentication failures.

dot1x-logoff: Specifies notifications about 802.1X user logoffs.

dot1x-logon: Specifies notifications about 802.1X authentication successes.

intrusion: Specifies notifications about illegal frame detection.

mac-auth-failure: Specifies notifications about MAC authentication failures.

mac-auth-logoff: Specifies notifications about MAC authentication user logoffs.

mac-auth-logon: Specifies notifications about MAC authentication successes.

Usage guidelines

To report critical port security events to an NMS, enable SNMP notifications for port security. For port security event notifications to be sent correctly, you must also configure SNMP on the device. For more information about SNMP configuration, see *Network Management and Monitoring Configuration Guide*.

If you do not specify a notification, this command enables all SNMP notifications for port security.

For this command to take effect, make sure the intrusion protection feature is configured.

Examples

Enable SNMP notifications about MAC address learning.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable port-security address-learned
```

Related commands

display port-security

port-security enable

Contents

User profile commands

display user-profile

Use **display user-profile** to display configuration and online user information for user profiles.

Syntax

display user-profile [**name** *profile-name*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *profile-name*: Specifies a user profile by its name, a case-sensitive string of 1 to 31 characters. Valid characters include English letters, digits, and underscores (_). The name must start with an English letter and must be unique. If you do not specify this option, the command displays configuration and online user information for all user profiles.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays user profile configuration and online user information for all member devices.

Examples

Display configuration and online user information for user profile **aaa**.

```
<Sysname> display user-profile name aaa
  User-Profile: aaa
    Inbound:
      Policy: p1

    User user_1:
      Authentication type: 802.1X
      Network attributes:
        Interface    : GigabitEthernet1/0/1
        MAC address  : 0000-1111-2222
      Failed action list:
        Inbound: Policy p1
```

Table 1 Command output

Field	Description
User-Profile	User profile name.
Inbound	Policy applied to incoming traffic.
Outbound	Policy applied to outgoing traffic.
Policy	Policy name.

Field	Description
User user_1	Username of a user account with which a user profile is associated.
Authentication type	Authentication type: • **802.1X**—802.1X authentication. • **Portal**—Portal authentication. • **MACA**—MAC authentication.
Network attributes	Online user information.
Failed action list	Actions that failed to be applied to the user.

user-profile

Use **user-profile** to create a user profile and enter its view, or enter the view of an existing user profile.

Use **undo user-profile** to delete a user profile.

Syntax

user-profile *profile-name*

undo user-profile *profile-name*

Default

No user profiles exist.

Views

System view

Predefined user roles

network-admin

Parameters

profile-name: Specifies a user profile by its name, a case-sensitive string of 1 to 31 characters. A user profile name can only contain English letters, digits, and underscores (_), and it must start with an English letter. The name must be unique.

Examples

Create user profile **a123** and enter the view of **a123**.

```
<Sysname> system-view
[Sysname] user-profile a123
[Sysname-user-profile-a123]
```

Contents

Password control commands

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

display password-control

Use **display password-control** to display password control configuration.

Syntax

display password-control [**super**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

super: Displays the password control information for the super passwords. If you do not specify this keyword, the command displays the global password control configuration.

Examples

Display the global password control configuration.

```
<Sysname> display password-control
 Global password control configurations:
Password control:                    Enabled (device management users)
                                     Enabled (network access users)
 Password aging:                      Enabled (90 days)
 Password length:                     Enabled (10 characters)
 Password composition:                Enabled (1 types, 1 characters per type)
 Password history:                    Enabled (max history records:4)
 Early notice on password expiration:  7 days
 Maximum login attempts:              3
 User authentication timeout:         600 seconds
 Action for exceeding login attempts:  Lock user for 1 minutes
 Password history was last reset:     0 days ago (device management users)
                                      0 days ago (network access users)
 Minimum interval between two updates: 24 hours
 User account idle time:              90 days
 Logins with aged password:           3 times in 30 days
 Password complexity:                 Disabled (username checking)
                                      Disabled (repeated characters checking)
 Password change:                     Enabled (first login)
                                      Enabled (mandatory weak password change)
```

Display the password control configuration for super passwords.

```
<Sysname> display password-control super
```

```
Super password control configurations:
Password aging:                         Enabled (90 days)
Password length:                        Enabled (10 characters)
Password composition:                   Enabled (1 types, 1 characters per type)
```

Table 1 Command output

Field	Description
Password control	Whether the password control feature is enabled for device management or network access users.
Password aging	Whether password expiration is enabled and, if enabled, the aging time.
Password length	Whether the minimum password length restriction feature is enabled and, if enabled, the setting.
Password composition	Whether the password composition restriction feature is enabled and, if enabled, the settings.
Password history	Whether the password history management feature is enabled and, if enabled, the setting.
Early notice on password expiration	Number of days during which the user is notified of the pending password expiration.
User authentication timeout	User authentication timeout time.
Maximum login attempts	Allowed maximum number of consecutive failed login attempts for FTP and VTY users.
Action for exceeding login attempts	Action to be taken after a user fails to log in after the specified number of attempts.
Password history was last reset	Last time when the password history records of the device management or network access users were deleted.
Minimum interval between two updates	Minimum password update interval.
Logins with aged password	Number of times and maximum number of days a user can log in using an expired password.
Password complexity	Whether the following password complexity checking is enabled: • **username checking**—Checks whether a password contains the username or the reverse of the username. • **repeated characters checking**—Checks whether a password contains any character that appears consecutively three or more times.
Password change	Status of the password change at first login feature: • Enabled (first login). • Disabled (first login). • Enabled (mandatory weak password change). • Disabled (mandatory weak password change).

display password-control blacklist

Use **display password-control blacklist** to display password control blacklist information.

Syntax

display password-control blacklist [**user-name** *user-name* | **ip** *ipv4-address* | **ipv6** *ipv6-address*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

user-name *user-name*: Specifies a user by its username, a case-sensitive string of 1 to 55 characters.

ip *ipv4-address*: Specifies the IPv4 address of a user.

ipv6 *ipv6-address*: Specifies the IPv6 address of a user.

Usage guidelines

If you do not specify any parameters, this command displays information about all users in the password control blacklist.

The users' IP addresses and user accounts are added to the password control blacklist when the users fail authentication. You can use this command to view information about blacklisted FTP, Web, and virtual terminal line (VTY) users.

Users accessing the system through the console interface are not blacklisted for the following reasons:

- The system is unable to obtain the IP addresses of these users.
- These users are privileged and, therefore, relatively secure to the system.

Examples

Display password control blacklist information.

```
<Sysname> display password-control blacklist
 Blacklist items matched: 2.
 Username                    IP address          Login failures   Lock flag
 abcd                        169::168:34:1       4                lock
 admin                       192.168.34.1        1                unlock
```

Table 2 Command output

Field	Description
Blacklist items matched	Number of blacklisted users.
IP address	IP address of the user.
Login failures	Number of login failures.
Lock flag	Whether the user account is locked for the user: • **unlock**—Not limited. • **lock**—Disabled temporarily or permanently, depending on the **password-control login-attempt** command.

password-control { aging | composition | history | length } enable

Use **password-control** { **aging** | **composition** | **history** | **length** } **enable** to enable a password restriction feature.

Use **undo password-control** { **aging** | **composition** | **history** | **length** } **enable** to disable a password restriction feature.

Syntax

password-control { **aging** | **composition** | **history** | **length** } **enable**

undo password-control { **aging** | **composition** | **history** | **length** } **enable**

Default

The password restriction features are all enabled.

Views

System view

Predefined user roles

network-admin

Parameters

aging: Enables the password expiration feature.

composition: Enables the password composition restriction.

history: Enables the password history management feature.

length: Enables the minimum password length restriction.

Usage guidelines

In versions earlier than Release 6318P01:

- For a specific password restriction setting to take effect, make sure you enable both the global password control and the specific password restriction. For example, if the global password control and the minimum length restriction feature are not enabled, the **password-control length** command does not take effect.
- If the global password control feature is enabled, the following rules apply:
  - In non-FIPS mode, a password must contain a minimum of 4 characters and a minimum of 4 characters must be different.
  - In FIPS mode, a password must contain a minimum of 15 characters and a minimum of 4 characters must be different.

In Release 6318P01 and later:

- The password expiration feature or the password history management feature takes effect only after the global password control is also enabled.
- In non-FIPS mode, the password composition restriction and the minimum password length restriction are enabled by default regardless of whether or not the global password control feature is enabled. The default minimum password length and default password composition restriction vary by device model.
- In FIPS mode, the password composition restriction or the minimum password length restriction takes effect only after the global password control is also enabled. When the password composition restriction takes effect, a password, by default, must contain a minimum of 4 different characters. When the minimum password length restriction takes effect, a password, by default, must contain a minimum of 15 characters.

If a password of a device management user is in hashed form, a restriction setting does not take effect for the password even when the following requirements are met:

- The global password control is enabled.
- The specific password restriction feature is enabled.

For more information about configuring a password for a device management user, see "AAA commands."

If the password history management feature is disabled, the system will not compare the new password with history passwords, but the system will not stop recording history passwords. When the number of history password records of a user reaches the maximum number set by the **password-control history** command, the newest history record overwrites the earliest one.

Examples

Enable the password control feature globally.

```
<Sysname> system-view
[Sysname] password-control enable
```

Enable the password composition restriction feature.

```
[Sysname] password-control composition enable
```

Enable the password expiration feature.

```
[Sysname] password-control aging enable
```

Enable the minimum password length restriction feature.

```
[Sysname] password-control length enable
```

Enable the password history management feature.

```
[Sysname] password-control history enable
```

Related commands

display password-control

password-control enable

password-control aging

Use **password-control aging** to set the password aging time.

Use **undo password-control aging** to restore the default.

Syntax

password-control aging *aging-time*

undo password-control aging

Default

A password expires after 90 days. The password aging time for a user group equals the global setting. The password aging time for a local user equals that of the user group to which the local user belongs.

Views

System view

User group view

Local user view

Predefined user roles

network-admin

Parameters

aging-time: Specifies the password aging time in days, in the range of 1 to 365.

Usage guidelines

The aging time depends on the view:

- The time in system view has global significance and applies to all user groups.
- The time in user group view applies to all local users in the user group.
- The time in local user view applies only to the local user.

A password aging time with a smaller application scope has higher priority. The system prefers to use the password aging time in local user view for a local user.

- If no password aging time is configured for the local user, the system uses the password aging time for the user group to which the local user belongs.
- If no password aging time is configured for the user group, the system uses the global password aging time.

Examples

Globally set the passwords to expire after 80 days.

```
<Sysname> system-view
[Sysname] password-control aging 80
```

Set the passwords for user group **test** to expire after 90 days.

```
[Sysname] user-group test
[Sysname-ugroup-test] password-control aging 90
[Sysname-ugroup-test] quit
```

Set the password for device management user **abc** to expire after 100 days.

```
[Sysname] local-user abc class manage
[Sysname-luser-manage-abc] password-control aging 100
```

Related commands

display local-user

display password-control

display user-group

password-control aging enable

password-control alert-before-expire

Use **password-control alert-before-expire** to set the number of days before a user's password expires during which the user is notified of the pending password expiration.

Use **undo password-control alert-before-expire** to restore the default.

Syntax

password-control alert-before-expire *alert-time*

undo password-control alert-before-expire

Default

The default is 7 days.

Views

System view

Predefined user roles

network-admin

Parameters

alert-time: Specifies the number of days before a user password expires during which the user is notified of the pending password expiration. The value range is 1 to 30.

Usage guidelines

This command is effective only for non-FTP users. FTP users can only have their passwords changed by the administrator.

Examples

Configure the device to notify a user about pending password expiration 10 days before the user's password expires.

```
<Sysname> system-view
[Sysname] password-control alert-before-expire 10
```

Related commands

display password-control

password-control authentication-timeout

Use **password-control authentication-timeout** to set the user authentication timeout time.

Use **undo password-control authentication-timeout** to restore the default.

Syntax

password-control authentication-timeout *timeout*

undo password-control authentication-timeout

Default

The user authentication timeout time is 600 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

timeout: Specifies the user authentication timeout time in seconds, in the range of 30 to 600.

Usage guidelines

This command takes effect only on Telnet and terminal users. When the authentication for a user times out, the connection will be terminated.

Examples

Set the user authentication timeout time to 40 seconds.

```
<Sysname> system-view
[Sysname] password-control authentication-timeout 40
```

Related commands

display password-control

password-control change-password first-login enable

Use **password-control change-password first-login enable** to enable the password change at first login feature.

Use **undo password-control change-password first-login enable** to disable the password change at first login feature.

Syntax

password-control change-password first-login enable

undo password-control change-password first-login enable

Default

The password change at first login feature is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

For the password change at first login feature to take effect, make sure the global password control and password change features are both enabled.

In FIPS mode, the password change at first login feature cannot be disabled.

Examples

Enable password change at first login.

```
<Sysname> system-view
[Sysname] password-control change-password first-login enable
```

Related commands

display password-control

password-control enable

password-control change-password weak-password enable

Use **password-control change-password weak-password enable** to enable mandatory weak password change.

Use **undo password-control change-password weak-password enable** to disable mandatory weak password change.

Syntax

password-control change-password weak-password enable

undo password-control change-password weak-password enable

Default

The mandatory weak password change feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command is available only in Release 6318P01 and later.

The system checks for weak login passwords for Telnet, SSH, HTTP, or HTTPS device management users. A password is weak if it does not meet the following requirements:

- Password composition restriction.
- Minimum password length restriction.
- Password complexity checking policy.

By default, the system displays a message about a weak password but does not force the user to change it. To improve the device security, you can enable the mandatory weak password change feature, which forces the users to change the identified weak passwords. The users can log in to the device only after their passwords meet the password requirements.

To view the password requirements, use the **display password-control** command. To change the password composition restriction, the minimum password length, and the password complexity checking policy, use the **password-control composition**, **password-control length**, and **password-control complexity** commands, respectively.

Examples

Enable the mandatory weak password change feature.

```
<Sysname> system-view
[Sysname] password-control change-password weak-password enable
```

Related commands

display password-control

password-control { **aging** | **composition** | **history** | **length** }

password-control complexity

password-control composition

password-control length

password-control enable

password-control complexity

Use **password-control complexity** to configure the password complexity checking policy.

Use **undo password-control complexity** to remove a password complexity checking item.

Syntax

password-control complexity { **same-character** | **user-name** } **check**

undo password-control complexity { **same-character** | **user-name** } **check**

Default

In versions earlier than Release 6318P01:

The global password complexity checking policy is that both username checking and repeated character checking are disabled. The password complexity checking policy for a user group equals the global setting. The password complexity checking policy for a local user equals that of the user group to which the local user belongs.

In Release 6318P01 and later:

- In non-FIPS mode:

  The global password complexity checking policy is that username checking is enabled and repeated character checking is disabled. The password complexity checking policy for a user group equals the global setting. The password complexity checking policy for a local user equals that of the user group to which the local user belongs.

- In FIPS mode:

  The global password complexity checking policy is that both username checking and repeated character checking are disabled. The password complexity checking policy for a user group equals the global setting. The password complexity checking policy for a local user equals that of the user group to which the local user belongs.

Views

System view

User group view

Local user view

Predefined user roles

network-admin

Parameters

`same-character`: Refuses a password that contains a minimum of three consecutive identical characters. For example, the password **aaabc** is not complex enough.

`user-name`: Refuses a password that contains the username or the reverse of the username. For example, if the username is **123**, a password such as **abc123** or **321df** is not complex enough.

Usage guidelines

The password complexity checking policy depends on the view:

- The policy in system view has global significance and applies to all user groups.
- The policy in user group view applies to all local users in the user group.
- The policy in local user view applies only to the local user.

A password complexity checking policy with a smaller application scope has higher priority. The system prefers to use the password complexity checking policy in local user view for a local user.

- If no policy is configured for the local user, the system uses the policy for the user group to which the local user belongs.
- If no policy is configured for the user group, the system uses the global policy.

In versions earlier than Release 6318P01, the password complexity checking is disabled. The password complexity checking takes effect only after you enable the global password control feature and execute the **`password-control complexity`** command.

In Release 6318P01 and later:

- In non-FIPS mode, username checking is enabled regardless of whether or not the global password control feature is enabled.
- In FIPS mode, the password complexity checking is disabled. The password complexity checking takes effect only after you enable the global password control feature and execute the **`password-control complexity`** command.

You can enable both username checking and repeated character checking.

Examples

Configure the password complexity checking policy, refusing any password that contains the username or the reverse of the username.

```
<Sysname> system-view
```

```
[Sysname] password-control complexity user-name check
```

Related commands

display local-user

display password-control

display user-group

password-control composition

Use **password-control composition** to configure the password composition policy.

Use **undo password-control composition** to restore the default.

Syntax

password-control composition type-number *type-number* [**type-length** *type-length*]

undo password-control composition

Default

In non-FIPS mode:

- In versions earlier than Release 6318P01, the password using the global composition policy must contain a minimum of one character type and a minimum of one character for each type.
- In Release 6318P01 and later, the password using the global composition policy must contain a minimum of two character types and a minimum of one character for each type.

In FIPS mode:

The password using the global composition policy must contain a minimum of four character types and a minimum of one character for each type.

In both non-FIPS and FIPS modes:

The password composition policy for a user group is the same as the global policy. The password composition policy for a local user is the same as that of the user group to which the local user belongs.

Views

System view

User group view

Local user view

Predefined user roles

network-admin

Parameters

type-number *type-number*: Specifies the minimum number of character types that a password must contain. The value range for the *type-number* argument is 1 to 4 in non-FIPS mode and fixed at 4 in FIPS mode.

type-length *type-length*: Specifies the minimum number of characters that are from each type in the password. The value range for the *type-length* argument is 1 to 63 in non-FIPS mode, and 1 to 15 in FIPS mode.

Usage guidelines

The password composition policy depends on the view:

- The policy in system view has global significance and applies to all user groups.

- The policy in user group view applies to all local users in the user group.
- The policy in local user view applies only to the local user.

A password composition policy with a smaller application scope has higher priority. The system prefers to use the password composition policy in local user view for a local user.

- If no policy is configured for the local user, the system uses the policy for the user group to which the local user belongs.
- If no policy is configured for the user group, the system uses the global policy.

The product of the minimum number of character types and minimum number of characters for each type cannot be greater than the maximum length of passwords.

Examples

Specify that all passwords must each contain a minimum of four character types and a minimum of five characters for each type.

```
<Sysname> system-view
[Sysname] password-control composition type-number 4 type-length 5
```

Specify that passwords in user group **test** must contain a minimum of four character types and a minimum of five characters for each type.

```
[Sysname] user-group test
[Sysname-ugroup-test] password-control composition type-number 4 type-length 5
[Sysname-ugroup-test] quit
```

Specify that the password of device management user **abc** must contain a minimum of four character types and a minimum of five characters for each type.

```
[Sysname] local-user abc class manage
[Sysname-luser-manage-abc] password-control composition type-number 4 type-length 5
```

Related commands

display local-user

display password-control

display user-group

password-control composition enable

password-control enable

Use **password-control enable** to enable the password control feature globally.

Use **undo password-control enable** to disable the password control feature globally.

Syntax

password-control enable [**network-class**]

undo password-control enable [**network-class**]

Default

In non-FIPS mode:

The password control feature is disabled globally for device management and network access users.

In FIPS mode:

The password control feature is enabled globally and cannot be disabled for device management users.

The password control feature is disabled globally for network access users.

Views

System view

Predefined user roles

network-admin

Parameters

network-class: Enables global password control for network access users. If you do not specify this keyword, the command enables global password control for device management users.

Usage guidelines

When you enable global password control, the device automatically generates a .dat file and saves the file to the storage media. The file is used to record authentication and login information of local users. Do not manually delete or modify the file.

In versions earlier than Release 6318P01:

A specific password control feature (password expiration, minimum password length, password history management, and password composition restriction) takes effect only after the global password control feature is enabled.

In Release 6318P01 and later versions:

The password expiration feature and the password history management feature take effect only after the global password control feature is also enabled.

After the global password control feature is enabled, the passwords configured for local users must contain a minimum of four different characters.

After the global password control feature is enabled for device management users, you cannot display the password and super password configuration for device management users by using the corresponding **display** commands.

After the global password control feature is enabled for network access users, you cannot display the password configuration for network access users by using the corresponding **display** commands.

You can configure all password control features for device management users.

You can configure only the following password control features for network access users:

- Password complexity checking policy.
- Password composition policy.
- Minimum password length.
- Minimum password update interval.
- Maximum number of history password records for each user.

Examples

Enable the password control feature globally for device management users.

```
<Sysname> system-view
[Sysname] password-control enable
```

Enable the password control feature globally for network access users.

```
<Sysname> system-view
[Sysname] password-control enable network-class
```

Related commands

display password-control

password-control complexity

password-control { **composition** | **history** | **length** } **enable**

password-control update-interval

password-control expired-user-login

Use **password-control expired-user-login** to set the maximum number of days and maximum number of times that a user can log in after the password expires.

Use **undo password-control expired-user-login** to restore the defaults.

Syntax

password-control expired-user-login delay *delay* **times** *times*

undo password-control expired-user-login

Default

A user can use an expired password to log in three times within 30 days after the password expires. If all three attempts fail or the user makes a login attempt after 30 days, the system prompts the user to set a new password.

Views

System view

Predefined user roles

network-admin

Parameters

delay *delay*: Specifies the maximum number of days during which a user can log in using an expired password. The value range for the *delay* argument is 1 to 90.

times *times*: Specifies the maximum number of times a user can log in after the password expires. The value range is 0 to 10. For a user to set a new password at the system prompt immediately after the password expires, set the value to 0.

Usage guidelines

This command is effective only on non-FTP login users. An FTP user cannot continue to log in after its password expires.

Examples

Allow a user to log in five times within 60 days after the password expires.

```
<Sysname> system-view
[Sysname] password-control expired-user-login delay 60 times 5
```

Related commands

display password-control

password-control history

Use **password-control history** to set the maximum number of history password records for each user.

Use **undo password-control history** to restore the default.

Syntax

password-control history *max-record-number*

undo password-control history

Default

The maximum number of history password records for each user is 4.

Views

System view

Predefined user roles

network-admin

Parameters

max-record-number: Specifies the maximum number of history password records for each user. The value range is 2 to 15.

Usage guidelines

The global password control feature enables the system to record history passwords. When the number of history password records of a user reaches the maximum number, the newest history record overwrites the earliest one.

To delete the existing records, use one of the following methods:

- Use the **undo password-control enable** command to disable the password control feature globally.
- Use the **reset password-control history-record** command to clear the passwords manually.

Examples

Set the maximum number of history password records for each user to 10.

```
<Sysname> system-view
[Sysname] password-control history 10
```

Related commands

display password-control

password-control history enable

reset password-control blacklist

password-control length

Use **password-control length** to set the minimum password length.

Use **undo password-control length** to restore the default.

Syntax

password-control length *length*

undo password-control length

Default

In non-FIPS mode:

The global minimum password length is 10 characters.

In FIPS mode:

The global minimum password length is 15 characters.

In both non-FIPS and FIPS modes:

The minimum password length for a user group equals the global setting. The minimum password length for a local user equals that of the user group to which the local user belongs.

Views

System view

User group view

Local user view

Predefined user roles

network-admin

Parameters

length: Specifies the minimum password length in characters. The value range for this argument is 4 to 32 in non-FIPS mode, and 15 to 32 in FIPS mode.

Usage guidelines

The minimum length setting depends on the view:

- The setting in system view has global significance and applies to all user groups.
- The setting in user group view applies to all local users in the user group.
- The setting in local user view applies only to the local user.

A minimum password length with a smaller application scope has higher priority. The system prefers to use the minimum password length in local user view for a local user.

- If no minimum password length is configured for the local user, the system uses the minimum password length for the user group to which the local user belongs.
- If no minimum password length is configured for the user group, the system uses the global minimum password length.

Examples

Set the global minimum password length to 16 characters.

```
<Sysname> system-view
[Sysname] password-control length 16
```

Set the minimum password length to 16 characters for the user group **test**.

```
[Sysname] user-group test
[Sysname-ugroup-test] password-control length 16
[Sysname-ugroup-test] quit
```

Set the minimum password length to 16 characters for the device management user **abc**.

```
[Sysname] local-user abc class manage
[Sysname-luser-manage-abc] password-control length 16
```

Related commands

display local-user

display password-control

display user-group

password-control length enable

password-control login idle-time

Use **password-control login idle-time** to set the maximum account idle time.

Use **undo password-control login idle-time** to restore the default.

Syntax

password-control login idle-time *idle-time*

undo password-control login idle-time

Default

The maximum account idle time is 90 days.

Views

System view

Predefined user roles

network-admin

Parameters

idle-time: Specifies the maximum account idle time in days. The value range is 0 to 365. 0 means no restriction for account idle time.

Usage guidelines

If a user account is idle for this period of time, the account becomes invalid and can no longer be used to log in to the device.

The account might become invalid if the system time changes after your last successful login. You cannot use an invalid account to log in. To disable the account idle time restriction, set the idle time value to 0.

Examples

Set the maximum account idle time to 30 days.

```
<Sysname> system-view
[Sysname] password-control login idle-time 30
```

Related commands

display password-control

password-control login-attempt

Use **password-control login-attempt** to configure the login attempt limit. The settings include the maximum number of consecutive login failures and the action to be taken when the maximum number is reached.

Use **undo password-control login-attempt** to restore the default.

Syntax

password-control login-attempt *login-times* [**exceed** { **lock** | **lock-time** *time* | **unlock** }]

undo password-control login-attempt

Default

The global login-attempt settings:

- The maximum number of consecutive login failures is 3.
- The locking period is 1 minute.

The login-attempt settings for a user group equal the global settings.

The login-attempt settings for a local user equal those for the user group to which the local user belongs.

Views

System view

User group view

Local user view

Predefined user roles

network-admin

Parameters

login-times: Specifies the maximum number of consecutive login failures. The value range is 2 to 10.

exceed: Specifies an action to be taken for the user who fails to log in after making the maximum number of attempts.

- **lock**: Disables the user account permanently.
- **lock-time** *time*: Disables the user account for a period of time. The user can uses this user account when the timer expires. The value range for the *time* argument is 1 to 360 minutes.
- **unlock**: Allows the user account to continue using this account to perform login attempts.

Usage guidelines

The login-attempt policy depends on the view:

- The policy in system view has global significance and applies to all user groups.
- The policy in user group view applies to all local users in the user group.
- The policy in local user view applies only to the local user.

A login-attempt policy with a smaller application scope has higher priority. The system prefers to use the login-attempt policy in local user view for a local user.

- If no policy is configured for the local user, the system uses the policy for the user group to which the local user belongs.
- If no policy is configured for the user group, the system uses the global policy.

If an FTP or VTY user fails to log in, the system adds the user account and the user's IP address to the password control blacklist. When the maximum number of consecutive login failures is reached, the login attempt limit feature is triggered.

Whether a blacklisted user and user account are locked depends on the locking setting:

- If a user account is permanently locked for a user, the user cannot use this account unless this account is removed from the password control blacklist. To remove the user account, use the **reset password-control blacklist** command.
- To use a temporarily locked user account, the user can perform either of the following tasks:
  - Wait until the locking timer expires.
  - Remove the user account from the password control blacklist.
- If the user account and the user are blacklisted but not locked, the user can continue using this account to log in. The account and the user's IP address are removed from the password control blacklist when the user uses the account to successfully log in to the device.

NOTE:

This account is locked only for this user. Other users can still use this account, and the blacklisted user can use other user accounts.

The **password-control login-attempt** command takes effect immediately after being executed, and can affect the users already in the password control blacklist.

Examples

Allow a maximum of four consecutive login failures on a user account, and disable the user account if the limit is reached.

```
<Sysname> system-view
[Sysname] password-control login-attempt 4 exceed lock
```

Use the user account **test** to log in to the device, and enter incorrect password for four times.

Display the password control blacklist. The output shows that the user account is on the blacklist, and its status is **lock**.

```
[Sysname] display password-control blacklist

 Username: test
    IP: 192.168.44.1        Login failures: 4      Lock flag: lock

 Blacklist items matched: 1.
```

Verify that the user at 192.168.44.1 cannot use this user account to log in.

Allow a maximum of two consecutive login failures on a user account, and disable the account for 3 minutes if the limit is reached.

```
<Sysname> system-view
[Sysname] password-control login-attempt 2 exceed lock-time 3
```

Use the user account **test** to log in to the device, and enter incorrect password for two attempts.

Display the password control blacklist. The output shows that the user account is on the blacklist and its status is **lock**.

```
[Sysname] display password-control blacklist

 Username: test
    IP: 192.168.44.1        Login failures: 2      Lock flag: lock

 Blacklist items matched: 1.
```

Verify that after 3 minutes, the user account is removed from the password control blacklist and the user at 192.168.44.1 can use this account.

Related commands

display local-user

display password-control

display password-control blacklist

display user-group

reset password-control blacklist

password-control super aging

Use **password-control super aging** to set the aging time for super passwords.

Use **undo password-control super aging** to restore the default.

Syntax

password-control super aging *aging-time*

undo password-control super aging

Default

A super password expires after 90 days.

Views

System view

Predefined user roles

network-admin

Parameters

aging-time: Specifies the super password aging time in days, in the range of 1 to 365.

Examples

Set the super passwords to expire after 10 days.

```
<Sysname> system-view
[Sysname] password-control super aging 10
```

Related commands

display password-control

password-control aging

password-control super composition

Use **password-control super composition** to configure the composition policy for super passwords.

Use **undo password-control super composition** to restore the default.

Syntax

password-control super composition type-number *type-number* [**type-length** *type-length*]

undo password-control super composition

Default

In non-FIPS mode:

- In versions earlier than Release 6318P01, a super password must contain a minimum of one character type and a minimum of one character for each type.
- In Release 6318P01 and later, a super password must contain a minimum of two character types and a minimum of one character for each type.

In FIPS mode:

A super password must contain a minimum of four character types and a minimum of one character for each type.

Views

System view

Predefined user roles

network-admin

Parameters

type-number *type-number*: Specifies the minimum number of character types that a super password must contain. The value range for the *type-number* argument is 1 to 4 in non-FIPS mode and fixed at 4 in FIPS mode.

type-length *type-length*: Specifies the minimum number of characters that are from each character type. The value range for the *type-length* argument is 1 to 63 in non-FIPS mode, and 1 to 15 in FIPS mode.

Usage guidelines

The product of the minimum number of character types and minimum number of characters for each type cannot be greater than the maximum length of the super password.

Examples

Specify that a super password must contain a minimum of four character types and a minimum of five characters for each type.

```
<Sysname> system-view
[Sysname] password-control super composition type-number 4 type-length 5
```

Related commands

display password-control

password-control composition

password-control super length

Use **password-control super length** to set the minimum length for super passwords.

Use **undo password-control super length** to restore the default.

Syntax

password-control super length *length*

undo password-control super length

Default

In non-FIPS mode:

The minimum super password length is 10 characters.

In FIPS mode:

The minimum super password length is 15 characters.

Views

System view

Predefined user roles

network-admin

Parameters

length: Specifies the minimum length of super passwords in characters. The value range for this argument is 4 to 63 in non-FIPS mode, and 15 to 63 in FIPS mode.

Examples

Set the minimum length of super passwords to 16 characters.

```
<Sysname> system-view
[Sysname] password-control super length 16
```

Related commands

display password-control

password-control length

password-control update-interval

Use **password-control update-interval** to set the minimum password update interval, which is the minimum interval at which users can change their passwords.

Use **undo password-control update-interval** to restore the default.

Syntax

password-control update-interval *interval*

undo password-control update-interval

Default

The minimum password update interval is 24 hours.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the minimum password update interval in hours, in the range of 0 to 168. 0 means no requirements for password update interval.

Usage guidelines

The set minimum interval is not effective on a device management user who is prompted to change the password at the first login or after the password expires.

Examples

Set the minimum password update interval to 36 hours.

```
<Sysname> system-view
[Sysname] password-control update-interval 36
```

Related commands

display password-control

reset password-control blacklist

Use **reset password-control blacklist** to remove blacklisted users.

Syntax

reset password-control blacklist [**user-name** *user-name*]

Views

User view

Predefined user roles

network-admin

Parameters

user-name *user-name*: Specifies the username of a user account to be removed from the password control blacklist. The username is a case-sensitive string of 1 to 55 characters.

Usage guidelines

You can use this command to remove a user account that is blacklisted due to excessive login failures. Then the blacklisted user can use this user account to log in.

Examples

Remove the user account named **test** from the password control blacklist.

```
<Sysname> reset password-control blacklist user-name test
Are you sure to delete the specified user in blacklist? [Y/N]:
```

Related commands

display password-control blacklist

reset password-control history-record

Use **reset password-control history-record** to delete history password records.

Syntax

reset password-control history-record [**super** [**role** *role-name*] | **user-name** *user-name* | **network-class** [**user-name** *user-name*]]

Views

User view

Predefined user roles

network-admin

Parameters

super: Deletes the history records of the specified super password or all super passwords.

role *role name*: Specifies a user role name, a case-sensitive string of 1 to 63 characters. If you do not specify this option, the command deletes the history records of all super passwords.

network-class: Deletes the history password records of network access users. If you do not specify this keyword, the command deletes the history password records of device management users.

user-name *user-name*: Specifies the username of the user whose password records are to be deleted. The *user-name* argument is a case-sensitive string of 1 to 55 characters. If you do not specify this option, the command deletes all history password records of the specified user type.

Usage guidelines

If you do not specify any parameters, this command deletes the history password records of all local users.

Examples

Delete the history password records of all device management users.

```
<Sysname> reset password-control history-record
Are you sure you want to delete all device management users' history records? [Y/N]:y
```

Delete the history password records of all network access users.

```
<Sysname> reset password-control history-record network-class
Are you sure you want to delete all network access users' history records? [Y/N]:y
```

Related commands

password-control history

Contents

Public key management commands

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

display public-key local public

Use **display public-key local public** to display local public keys.

Syntax

display public-key local { **dsa** | **ecdsa** | **rsa** } **public** [**name** *key-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

dsa: Specifies the DSA key pair type.

ecdsa: Specifies the ECDSA key pair type.

rsa: Specifies the RSA key pair type.

name *key-name*: Specifies a local key pair by its name, a case-insensitive string of 1 to 64 characters. Valid characters are letters, digits, and hyphens (-). If you do not specify a key pair, this command displays the public keys of all local key pairs of the specified type.

Usage guidelines

You can copy and distribute the public key of a local key pair to peer devices.

You cannot display a host public key that has the default key pair name by specifying the **name** *key-name* option. To view a host public key that has the default key pair name, display all local public keys by using this command without specifying a key pair name.

Examples

Display all local RSA public keys.

```
<Sysname> display public-key local rsa public

=============================================
Key name: hostkey (default)
Key type: RSA
Time when key pair created: 15:40:48 2011/05/12
Key code:
   30819F300D06092A864886F70D010101050003818D0030818902818100DAA4AAFEFE04C2C9
   667269BB8226E26331E30F41A8FF922C7338208097E84332610632B49F75DABF6D871B80CE
   C1BA2B75020077C74745C933E2F390DC0B39D35B88283D700A163BB309B19F8F87216A44AB
   FBF6A3D64DEB33E5CEBF2BCF26296778A26A84F4F4C5DBF8B656ACFA62CD96863474899BC1
   2DA4C04EF5AE0835090203010001
=============================================
```

```
Key name: serverkey (default)
Key type: RSA
Time when key pair created: 15:40:48 2011/05/12
Key code:
   307C300D06092A864886F70D0101010500036B003068026100CAB4CACCA16442AD5F453442
   762F03897E0D494FEDE69224F5C051A441D290976733A278C9F0C0F5A198E66143EAB54A64
   DB608269CAE844B1E7CC64AD7E808972E7CF887F3B657F056E7930FC84FBF1AD83A01CC47E
   9D85C13413996ECD093B0203010001
==========================================
Key name: rsa1
Key type: RSA
Time when key pair created: 15:42:26 2011/05/12
Key code:
   30819F300D06092A864886F70D010101050003818D003081890281810 0DEBC46F217DDF11D
   426E7095AA45CD6BF1F87343D952569AC223A01365E0D8C91D49D347C143C5D8FAADA896AA
   1A827E580F2502F1926F52197230E1DE391A64015C43DD79DC4E9E171BAEA1DEB4C71DAED7
   9A6EDFD460D8945D27D39B7C9822D56AEA5B7C2CCFF1B6BC524AD498C3B87D4BD6EB36AF03
   92D8C6D940890BF4290203010001
```

Display all local DSA public keys.

```
<Sysname> display public-key local dsa public

==========================================
Key name: dsakey (default)
Key type: DSA
Time when key pair created: 15:41:37 2011/05/12
Key code:
   308201B73082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
   96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
   DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
   DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
   7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
   4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
   35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
   91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
   585DA7F42519718CC9B09EEF038184000 2818041912CE34D12BCD2157E7AB1C2F03B3EF395
   100F3DB4A9E2FDFE860C1BD663D676438F7DA40A9406D61CA9079AF13E330489F1C76785DE
   52DA649AC8BC04B6D39CD7C52CD0A14F75F7491A91D31D6AC22340B5981B27A915CDEC4F09
   887E541EC1E5302D500F68E7AC29A084463C60F9EE266985A502FC92193E1CF4D265C4BA
==========================================
Key name: dsa1
Key type: DSA
Time when key pair created: 15:35:42 2011/05/12
Key code:
   308201B83082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
   96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
   DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
   DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
   7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
```

```
   4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
   35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
   91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
   585DA7F42519718CC9B09EEF0381850002818100A1E456C8DA2AD1BB83B1BDF2A1A6B5A6E8
   3642B460402445DA7E4036715F468F76655E114D460B7112F57143EE020AEF4A5BFAD07B74
   0FBCB1C64DA8A2BCE619283421445EEC77D3CF0D11866E9656AD6511F4926F8376967B0AB7
   15F9FB7B514BC1174155DD6E073B1FCB3A2749E6C5FEA81003E16729497D0EAD9105E3E76A
```

Display all local ECDSA public keys.

```
<Sysname> display public-key local ecdsa public

=============================================
Key name: ecdsakey (default)
Key type: ECDSA
Time when key pair created: 15:42:04 2011/05/12
Key code:
   3049301306072A8648CE3D020106082A8648CE3D03010103320004C10CF7CE42193F7FC2AF
   68F5DC877835A43009DB6135558A7FB8316C361B0690B4FD84A14C0779C76DD6145BF9362B
   1D
=============================================
Key name: ecdsa1
Key type: ECDSA
Time when key pair created: 15:43:33 2011/05/12
Key code:
   3049301306072A8648CE3D020106082A8648CE3D03010103320004A1FB84D92315B8DB72D1
   AE672C7CFA5135D5F5B02377F2F092F182EC83B5819795BC94CCBD3EBA7D4F0F2B2EB20C58
   4D
```

Display the public key of the local RSA key pair **rsa1**.

```
<Sysname> display public-key local rsa public name rsa1

=============================================
Key name: rsa1
Key type: RSA
Time when key pair created: 15:42:26 2011/05/12
Key code:
   30819F300D06092A864886F70D010101050003818D0030818902818100DEBC46F217DDF11D
   426E7095AA45CD6BF1F87343D952569AC223A01365E0D8C91D49D347C143C5D8FAADA896AA
   1A827E580F2502F1926F52197230E1DE391A64015C43DD79DC4E9E171BAEA1DEB4C71DAED7
   9A6EDFD460D8945D27D39B7C9822D56AEA5B7C2CCFF1B6BC524AD498C3B87D4BD6EB36AF03
   92D8C6D940890BF4290203010001
```

Display the public key of the local DSA key pair **dsa1**.

```
<Sysname> display public-key local dsa public name dsa1

=============================================
Key name: dsa1
Key type: DSA
Time when key pair created: 15:35:42 2011/05/12
Key code:
   308201B83082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
```

```
   96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
   DBD13EC8B274DA9F75BA26CCB9877236027 87E922BA84421F22C3C89CB9B06FD60FE01941D
   DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
   7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F028181008226900 9E1
   4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
   35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
   91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
   585DA7F42519718CC9B09EEF0381850002818100A1E456C8DA2AD1BB83B1BDF2A1A6B5A6E8
   3642B460402445DA7E4036715F468F76655E114D460B7112F57143EE020AEF4A5BFAD07B74
   0FBCB1C64DA8A2BCE619283421445EEC77D3CF0D11866E9656AD6511F4926F8376967B0AB7
   15F9FB7B514BC1174155DD6E073B1FCB3A2749E6C5FEA81003E16729497D0EAD9105E3E76A
```

Display the public key of the local ECDSA key pair **ecdsa1**.

```
<Sysname> display public-key local ecdsa public name ecdsa1

=========================================
Key name: ecdsa1
Key type: ECDSA
Time when key pair created: 15:43:33 2011/05/12
Key code:
   3049301306072A8648CE3D020106082A8648CE3D03010103320004A1FB84D92315B8DB72D1
   AE672C7CFA5135D5F5B02377F2F092F182EC83B5819795BC94CCBD3EBA7D4F0F2B2EB20C58
   4D
```

Table 1 Command output

Field	Description
Key name	Name of the local key pair. If you did not specify a name when creating the key pair, the default name is used followed by the word **default** in brackets. The following is the default key pair name for each key algorithm: • **hostkey**—Default RSA host key pair name. • **serverkey**—Default RSA server key pair name. • **dsakey**—Default DSA host key pair name. • **ecdsakey**—Default ECDSA host key pair name.
Key type	Options include: • RSA. • DSA. • ECDSA.
Time when key pair created	Date and time when the local key pair was created.
Key code	Public key string.

Related commands

`public-key local create`

display public-key peer

Use **`display public-key peer`** to display information about peer host public keys.

Syntax

display public-key peer [**brief** | **name** *publickey-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

brief: Displays brief information about all peer host public keys. The brief information includes only the key type, key modulus, and key name.

name *publickey-name*: Displays detailed information about a peer host public key, including its key code. The *publickey-name* argument specifies a peer host public by its name, a case-sensitive string of 1 to 64 characters.

Usage guidelines

If you do not specify any keywords, this command displays detailed information about all peer host public keys configured on the local device.

You can use the **public-key peer** command or the **public-key peer import sshkey** command to configure a peer host public key on the local device.

Examples

Display detailed information about the peer host public key **idrsa**.

```
<Sysname> display public-key peer name idrsa

=============================================
Key name: idrsa
Key type: RSA
Key modulus: 1024
Key code:
   30819F300D06092A864886F70D010101050003818D0030818902818100C5971581A78B5388
   B3C9063EC6B53D395A6704D9752B6F9B7B1F734EEB5DD509F0B050662C46FFB8D27F797E37
   918F6270C5793F1FC63638970A0E4D51A3CEF7CFF6E92BFAFD73F530E0BDE27056E81F2525
   6D0883836FD8E68031B2C272FE2EA75C87734A7B8F85B8EBEB3BD51CC26916AF3B3FDC32C3
   42C142D41BB4884FEB0203010001
```

Table 2 Command output

Field	Description
Key name	Name of the peer host public key.
Key type	Key type: RSA, DSA or ECDSA.
Key modulus	Key modulus length in bits.
Key code	Public key string.

Display brief information about all peer host public keys.

```
<Sysname> display public-key peer brief
Type  Modulus  Name
```

```
--------------------------
RSA   1024    idrsa
DSA   1024    10.1.1.1
```

Table 3 Command output

Field	Description
Type	Key type: RSA, DSA or ECDSA.
Modulus	Key modulus length in bits.
Name	Name of the peer host public key.

Related commands

public-key peer

public-key peer import sshkey

peer-public-key end

Use **peer-public-key end** to exit public key view to system view and save the configured peer host public key.

Syntax

peer-public-key end

Views

Public key view

Predefined user roles

network-admin

Usage guidelines

After you type the peer host public key on the local device, use this command to exit public key view and to save the peer host public key.

The system verifies the public key before saving it. If the key is not in the correct format, the system discards the key and displays an error message. If the key is valid, for example, the key was displayed by the **display public-key local public** command, the system saves the key.

Examples

Exit public key view and save the configured peer host public key.

```
<Sysname> system-view
[Sysname] public-key peer key1
Enter public key view. Return to system view with "peer-public-key end" command.
[Sysname-pkey-public-key-key1]30819F300D06092A864886F70D010101050003818D0030818902818
100C0EC8014F82515F6335A0A
[Sysname-pkey-public-key-key1]EF8F999C01EC94E5760A079BD73E4F4D97F3500EDB308C29481B77E
719D1643135877E13B1C531B4
[Sysname-pkey-public-key-key1]FF1877A5E2E7B1FA4710DB0744F66F6600EEFE166F1B854E2371D5B
952ADF6B80EB5F52698FCF3D6
[Sysname-pkey-public-key-key1]1F0C2EAAD9813ECB16C5C7DC09812D4EE3E9A0B074276FFD4AF2050
BD4A9B1DDE675AC30CB020301
[Sysname-pkey-public-key-key1]0001
```

```
[Sysname-pkey-public-key-key1] peer-public-key end
[Sysname]
```

Related commands

display public-key local public

display public-key peer

public-key peer

public-key local create

Use **public-key local create** to create local key pairs.

Syntax

In non-FIPS mode:

public-key local create { **dsa** | **ecdsa** [**secp192r1** | **secp256r1** | **secp384r1** | **secp521r1**] | **rsa** } [**name** *key-name*]

In FIPS mode:

public-key local create { **dsa** | **ecdsa** [**secp256r1** | **secp384r1** | **secp521r1**] | **rsa** } [**name** *key-name*]

Default

No local key pairs exist.

Views

System view

Predefined user roles

network-admin

Parameters

dsa: Specifies the DSA key pair type.

ecdsa: Specifies the ECDSA key pair type.

- **secp192r1**: Uses the secp192r1 curve to create a 192-bit ECDSA key pair.
- **secp256r1**: Uses the secp256r1 curve to create a 256-bit ECDSA key pair.
- **secp384r1**: Uses the secp384r1 curve to create a 384-bit ECDSA key pair.
- **secp521r1**: Uses the secp521r1 curve to create a 521-bit ECDSA key pair.

By default, the secp192r1 curve is used in non-FIPS mode and the secp256r1 curve is used in FIPS mode.

rsa: Specifies the RSA key pair type.

name *key-name*: Assigns a name to the key pair. The *key-name* argument is a case-insensitive string of 1 to 64 characters. Valid characters are letters, digits, and hyphens (-). If you do not assign a name to the key pair, the key pair takes the default name.

Table 4 Default local key pair names

Type	Default name
RSA	• Host key pair: **hostkey** • Server key pair: **serverkey**
DSA	**dsakey**

Type	Default name
ECDSA	**ecdsakey**

Usage guidelines

The key algorithm must be the same as required by the security application.

When you create an RSA or DSA key pair, enter an appropriate key modulus length at the prompt. The longer the key modulus length, the higher the security, and the longer the key generation time.

When you create an ECDSA key pair, choose the appropriate elliptic curve. The elliptic curve determines the ECDSA key length. The longer the key length, the higher the security, and the longer the key generation time.

See Table 5 for more information about key modulus lengths and key lengths.

If you do not assign the key pair a name, the system assigns the default name to the key pair and marks the key pair as **`default`**. You can also assign the default name to another key pair, but the system does not mark the key pair as **default**. The name of a key pair must be unique among all manually named key pairs that use the same key algorithm. If a name conflict occurs, the system asks whether you want to overwrite the existing key pair.

The key pairs are automatically saved and can survive system reboots.

Table 5 A comparison of different types of asymmetric key algorithms

Type	Generated key pairs	Modulus/key length

RSA	• In non-FIPS mode:
	  ◦ One host key pair, if you specify a key pair name.
	  ◦ One server key pair and one host key pair, if you do not specify a key pair name.
	  Both key pairs use their default names.
	• In FIPS mode: One host key pair.
	NOTE:
	Only SSH 1.5 uses the RSA server key pair.
		RSA key modulus length:
		• In non-FIPS mode: 512 to 4096 bits, 1024 bits by default.
		To ensure security, use a minimum of 768 bits.
		• In FIPS mode: A multiple of 256 bits in the range of 2048 to 4096 bits, 2048 bits by default.

DSA	One host key pair.	DSA key modulus length: • In non-FIPS mode: 512 to 2048 bits, 1024 bits by default. To ensure security, use a minimum of 768 bits. • In FIPS mode: 2048 bits.
ECDSA	One host key pair.	ECDSA key length: • In non-FIPS mode: 192, 256, 384, or 521 bits. • In FIPS mode: 256, 384, or 521 bits.

Examples

Create local RSA key pairs with default names.

```
<Sysname> system-view
[Sysname] public-key local create rsa
The range of public key modulus is (512 ~ 4096).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
```

```
Input the modulus length [default = 1024]:
Generating Keys...
....
Create the key pair successfully.
```

Create a local DSA key pair with the default name.

```
<Sysname> system-view
[Sysname] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
....
Create the key pair successfully.
```

Create a local ECDSA key pair with the default name.

```
<Sysname> system-view
[Sysname] public-key local create ecdsa
Generating Keys...
Create the key pair successfully.
```

Create a local RSA key pair with the name **rsa1**.

```
<Sysname> system-view
[Sysname] public-key local create rsa name rsa1
The range of public key modulus is (512 ~ 4096).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
..
Create the key pair successfully.
```

Create a local DSA key pair with the name **dsa1**.

```
<Sysname> system-view
[Sysname] public-key local create dsa name dsa1
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....
Create the key pair successfully.
```

Create a local ECDSA key pair with the name **ecdsa1**.

```
<Sysname> system-view
[Sysname] public-key local create ecdsa name ecdsa1
Generating Keys...
Create the key pair successfully.
```

In FIPS mode, create a local RSA key pair with the default name.

```
<Sysname> system-view
[Sysname] public-key local create rsa
```

```
The range of public key modulus is (2048 ~ 4096), a multiple of 256.
It will take a few minutes.Press CTRL+C to abort.
Input the modulus length [default = 2048]:
Generating Keys...
....
Create the key pair successfully.
```

In FIPS mode, create a local DSA key pair with the default name.

```
<Sysname> system-view
[Sysname] public-key local create dsa
The range of public key modulus is (2048 ~ 2048).
It will take a few minutes.Press CTRL+C to abort.
Input the modulus length [default = 2048]:
..
Create the key pair successfully.
```

Related commands

display public-key local public

public-key local destroy

public-key local destroy

Use **public-key local destroy** to destroy local key pairs.

Syntax

public-key local destroy { **dsa** | **ecdsa** | **rsa** } [**name** *key-name*]

Views

System view

Predefined user roles

network-admin

Parameters

dsa: Specifies the DSA key pair type.

ecdsa: Specifies the ECDSA key pair type.

rsa: Specifies the RSA key pair type.

name *key-name*: Specifies a local key pair by its name, a case-insensitive string of 1 to 64 characters. Valid characters are letters, digits, and hyphens (-). If you do not specify a key pair, this command destroys all key pairs of the specified type.

Usage guidelines

To avoid key compromise, destroy the local key pair and generate a new pair after any of the following conditions occurs:

- An intrusion event has occurred.
- The storage media of the device is replaced.
- The local certificate has expired. For more information about local certificates, see *Security Configuration Guide*.

Examples

Destroy the local RSA key pairs with the default names.

```
<Sysname> system-view
[Sysname] public-key local destroy rsa
Confirm to destroy the key pair? [Y/N]:y
```

Destroy the local DSA key pair with the default name.

```
<Sysname> system-view
[Sysname] public-key local destroy dsa
Confirm to destroy the key pair? [Y/N] :y
```

Destroy the local ECDSA key pair with the default name.

```
<Sysname> system-view
[Sysname] public-key local destroy ecdsa
Confirm to destroy the key pair? [Y/N]:y
```

Destroy the local RSA key pair **rsa1**.

```
<Sysname> system-view
[Sysname] public-key local destroy rsa name rsa1
Confirm to destroy the key pair? [Y/N]:y
```

Destroy the local DSA key pair **dsa1**.

```
<Sysname> system-view
[Sysname] public-key local destroy dsa name dsa1
Confirm to destroy the key pair? [Y/N] :y
```

Destroy the local ECDSA key pair **ecdsa1**.

```
<Sysname> system-view
[Sysname] public-key local destroy ecdsa name ecdsa1
Confirm to destroy the key pair? [Y/N]:y
```

Related commands

public-key local create

public-key local export dsa

Use **public-key local export dsa** to export a local DSA host public key.

Syntax

public-key local export dsa [**name** *key-name*] { **openssh** | **ssh2** } [*filename*]

Views

System view

Predefined user roles

network-admin

Parameters

name *key-name*: Specifies a local DSA key pair by its name, a case-insensitive string of 1 to 64 characters. Valid characters are letters, digits, and hyphens (-). If you do not specify a key pair, this command exports the host public key of the local DSA key pair with the default name.

openssh: Exports the host public key in OpenSSH format.

ssh2: Exports the host public key in SSH 2.0 format.

filename: Specifies the name of the file for saving the DSA host public key. The file name is a case-insensitive string of 1 to 128 characters. The name cannot be all dots (.), hostkey, serverkey, dsakey, or ecdsakey, and cannot start with a slash (/) or contain **./** and **../**. For more information about

file names, see *Fundamentals Configuration Guide*. If you do not specify a file name, this command displays the key on the monitor screen.

Usage guidelines

You can use this command to export a local DSA host public key before distributing it to a peer device.

To distribute a local DSA host public key to a peer device:

1. Save the exported local host public key to a file by using one of the following methods:
   - Use the **public-key local export dsa** [**name** *key-name*] { **openssh** | **ssh2** } command to export the local host public key, and then copy and paste the key to a file.
   - Use the **public-key local export dsa** [**name** *key-name*] { **openssh** | **ssh2** } *filename* command to export the key to a file. You cannot export the key to the folder **pkey** or its subfolders.
2. Transfer a copy of the file to the peer device, for example, by using FTP in binary mode or TFTP. For more information about FTP and TFTP, see *Fundamentals Configuration Guide*.
3. On the peer device, use the **public-key peer import sshkey** command to import the host public key from the file.

SSH 2.0 and OpenSSH are different public key formats. Choose the correct format that is supported on the device where you import the host public key.

Examples

Export the host public key of the local DSA key pair with the default name in OpenSSH format to a file named **key.pub**.

```
<Sysname> system-view
[Sysname] public-key local export dsa openssh key.pub
```

Display the host public key of the local DSA key pair with the default name in SSH 2.0 format.

```
<Sysname> system-view
[Sysname] public-key local export dsa ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "dsa-key-2011/05/12"
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5sJlhUiJ3
B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKNl/BnjXcitTQchQbz
WCFLFqL6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIEAgiaQCeFOxHS68pMuadOx8YU
XrZWUGEzN/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UILiLFs3ThbdABMs5xsCAhcJGscXthI5HH
bB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlxjMmwnu8AAACAQZEs400SvNIVfnqxw
vA7PvOVEA89tKni/f6GDBvWY9Z2Q499pAqUBtYcqQea8T4zBInxx2eF3lLaZJrIvAS205zXxSzQoU9190kakd
MdasIjQLWYGyepFc3sTwmIflQeweUwLVAPaOesKaCERjxg+e4maYWlAvySGT4c9NJlxLo=
---- END SSH2 PUBLIC KEY ----
```

Display the host public key of the local DSA key pair with the default name in OpenSSH format.

```
<Sysname> system-view
[Sysname] public-key local export dsa openssh
ssh-dss
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5sJlhUiJ3
B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKNl/BnjXcitTQchQbz
WCFLFqL6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIEAgiaQCeFOxHS68pMuadOx8YU
XrZWUGEzN/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UILiLFs3ThbdABMs5xsCAhcJGscXthI5HH
bB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlxjMmwnu8AAACAQZEs400SvNIVfnqxw
vA7PvOVEA89tKni/f6GDBvWY9Z2Q499pAqUBtYcqQea8T4zBInxx2eF3lLaZJrIvAS205zXxSzQoU9190kakd
MdasIjQLWYGyepFc3sTwmIflQeweUwLVAPaOesKaCERjxg+e4maYWlAvySGT4c9NJlxLo= dsa-key
```

Export the host public key of the local DSA key pair **dsa1** in OpenSSH format to the file **dsa1.pub**.

```
<Sysname> system-view
```

```
[Sysname] public-key local export dsa name dsa1 openssh dsa1.pub
```

Display the host public key of the local DSA key pair **dsa1** in SSH 2.0 format.

```
<Sysname> system-view
[Sysname] public-key local export dsa name dsa1 ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "dsa-key-2011/05/12"
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5sJlhUiJ3
B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKNl/BnjXcitTQchQbz
WCFLFqL6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIEAgiaQCeFOxHS68pMuadOx8YU
XrZWUGEzN/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UILiLFs3ThbdABMs5xsCAhcJGscXthI5HH
bB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlxjMmwnu8AAACBAKHkVsjaKtG7g7G98
qGmtaboNkK0YEAkRdp+QDZxX0aPdmVeEU1GC3ES9XFD7gIK70pb+tB7dA+8scZNqKK85hkoNCFEXux3088NEY
ZullatZRH0km+DdpZ7CrcV+ft7UUvBF0FV3W4HOx/LOidJ5sX+qBAD4WcpSX0OrZEF4+dq
---- END SSH2 PUBLIC KEY ----
```

Display the host public key of the local DSA key pair **dsa1** in OpenSSH format.

```
<Sysname> system-view
[Sysname] public-key local export dsa name dsa1 openssh
ssh-dss
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5sJlhUiJ3
B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKNl/BnjXcitTQchQbz
WCFLFqL6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIEAgiaQCeFOxHS68pMuadOx8YU
XrZWUGEzN/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UILiLFs3ThbdABMs5xsCAhcJGscXthI5HH
bB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlxjMmwnu8AAACBAKHkVsjaKtG7g7G98
qGmtaboNkK0YEAkRdp+QDZxX0aPdmVeEU1GC3ES9XFD7gIK70pb+tB7dA+8scZNqKK85hkoNCFEXux3088NEY
ZullatZRH0km+DdpZ7CrcV+ft7UUvBF0FV3W4HOx/LOidJ5sX+qBAD4WcpSX0OrZEF4+dq dsa-key
```

Related commands

public-key local create

public-key peer import sshkey

public-key local export ecdsa

Use **public-key local export ecdsa** to export a local ECDSA host public key.

Syntax

public-key local export ecdsa [**name** *key-name*] { **openssh** | **ssh2** } [*filename*]

Views

System view

Predefined user roles

network-admin

Parameters

name *key-name*: Specifies a local ECDSA key pair by its name, a case-insensitive string of 1 to 64 characters. Valid characters are letters, digits, and hyphens (-). If you do not specify a key pair, this command exports the host public key of the local ECDSA key pair with the default name.

openssh: Exports the host public key in OpenSSH format.

ssh2: Exports the host public key in SSH 2.0 format.

filename: Specifies the name of the file for saving the local host public key. The file name is a case-insensitive string of 1 to 128 characters. The name cannot be dots (.), hostkey, serverkey, dsakey, or ecdsakey, and cannot start with a slash (/) or contain ***./*** and ***../***. For more information about file names, see *Fundamentals Configuration Guide*. If you do not specify a file name, this command displays the key on the monitor screen.

Usage guidelines

You can use this command to export a local ECDSA host public key before distributing it to a peer device.

To distribute a local ECDSA host public key to a peer device:

1. Save the exported ECDSA host public key to a file by using one of the following methods:
   - Use the **public-key local export ecdsa** [**name** *key-name*] { **openssh** | **ssh2** } command to export the local host public key, and then copy and paste it to a file.
   - Use the **public-key local export ecdsa** [**name** *key-name*] { **openssh** | **ssh2** } *filename* command to export the host public key to a file. You cannot export the key to the folder **pkey** or its subfolders.
2. Transfer a copy of the file to the peer device, for example, by using FTP in binary mode or TFTP. For more information about FTP and TFTP, see *Fundamentals Configuration Guide*.
3. On the peer device, use the **public-key peer import sshkey** command to import the host public key from the file.

SSH 2.0 and OpenSSH are different public key formats. Choose the correct format that is supported by the device where you import the host public key.

Only the ECDSA host public key generated by using the secp256r1 curve can be exported.

Examples

Export the host public key of the local ECDSA key pair with the default name in OpenSSH format to the file named **key.pub**.

```
<Sysname> system-view
[Sysname] public-key local export ecdsa openssh key.pub
```

Display the host public key of the local ECDSA key pair with the default name in SSH 2.0 format.

```
<Sysname> system-view
[Sysname] public-key local export ecdsa ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "ecdsa-sha2-nistp256-2014/07/06"
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBREw5tkARpbV+sYArt/xcW+UJEAevx7O
ckTtTLPBiLP5bWkSdKbvo+3oHRuIyZqmNTIcxuBjuBap+pHc919C58=
---- END SSH2 PUBLIC KEY ----
```

Display the host public key of the local ECDSA key pair with the default name in OpenSSH format.

```
<Sysname> system-view
[Sysname] public-key local export ecdsa openssh
ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBREw5tkARpbV+sYArt/xcW+UJEAevx7O
ckTtTLPBiLP5bWkSdKbvo+3oHRuIyZqmNTIcxuBjuBap+pHc919C58=
 ecdsa-key
```

Related commands

public-key local create

public-key peer import sshkey

public-key local export rsa

Use **public-key local export rsa** to export a local RSA host public key.

Syntax

In non-FIPS mode:

public-key local export rsa [**name** *key-name*] { **openssh** | **ssh1** | **ssh2** } [*filename*]

In FIPS mode:

public-key local export rsa [**name** *key-name*] { **openssh** | **ssh2** } [*filename*]

Views

System view

Predefined user roles

network-admin

Parameters

name *key-name*: Specifies a local RSA key pair by its name, a case-insensitive string of 1 to 64 characters. Valid characters are letters, digits, and hyphens (-). If you do not specify a key pair, this command exports the host public key of the local RSA key pair with the default name.

openssh: Exports the host public key in OpenSSH format.

ssh1: Exports the host public key in SSH 1.5 format.

ssh2: Exports the host public key in SSH 2.0 format.

filename: Specifies the name of the file for saving the RSA host public key. The file name is a case-insensitive string of 1 to 128 characters. The name cannot be all dots (.), hostkey, serverkey, dsakey, or ecdsakey, and cannot start with a slash (/) or contain **./** and **../**. For more information about file names, see *Fundamentals Configuration Guide*. If you do not specify a file name, this command displays the key on the monitor screen.

Usage guidelines

You can use this command to export a local RSA host public key before distributing it to a peer device.

To distribute a local RSA host public key to a peer device:

1. Save the exported local host public key to a file by using one of the following methods:
   - Use the **public-key local export rsa** [**name** *key-name*] { **openssh** | **ssh2** } command to export the key, and then copy and paste it to a file.
   - Use the **public-key local export rsa** [**name** *key-name*] { **openssh** | **ssh2** } *filename* command to export key to a file. You cannot export the key to the folder **pkey** or its subfolders.
2. Transfer a copy of the file to the peer device, for example, by using FTP in binary mode or TFTP. For more information about FTP and TFTP, see *Fundamentals Configuration Guide*.
3. On the peer device, use the **public-key peer import sshkey** command to import the host public key from the file.

Choose the correct public key format that is supported on the device where you import the host public key. In FIPS mode, the device only supports SSH 2.0 and OpenSSH.

Examples

Export the host public key of the local RSA key pair with the default name in OpenSSH format to the file **key.pub**.

```
<Sysname> system-view
[Sysname] public-key local export rsa openssh key.pub
```

Display the host public key of the local RSA key pair with the default name in SSH 2.0 format.

```
<Sysname> system-view
[Sysname] public-key local export rsa ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-2011/05/12"
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDapKr+/gTCyWZyabuCJuJjMeMPQaj/kixzOCCAl+hDMmEGMrSfddq/b
YcbgM7Buit1AgB3x0dFyTPi85DcCznTW4goPXAKFjuzCbGfj4chakSr+/aj1k3rM+XOvyvPJilneKJqhPT0xd
v4tlas+mLNloY0dImbwS2kwE71rgg1CQ==
---- END SSH2 PUBLIC KEY ----
```

Display the host public key of the local RSA key pair with the default name in OpenSSH format.

```
<Sysname> system-view
[Sysname] public-key local export rsa openssh
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDapKr+/gTCyWZyabuCJuJjMeMPQaj/kixzOCCAl+hDMmEGMrSfddq/b
YcbgM7Buit1AgB3x0dFyTPi85DcCznTW4goPXAKFjuzCbGfj4chakSr+/aj1k3rM+XOvyvPJilneKJqhPT0xd
v4tlas+mLNloY0dImbwS2kwE71rgg1CQ== rsa-key
```

Export the host public key of the local RSA key pair **rsa1** in OpenSSH format to the file **rsa1.pub**.

```
<Sysname> system-view
[Sysname] public-key local export rsa name rsa1 openssh rsa1.pub
```

Display the host public key of the local RSA key pair **rsa1** in SSH 2.0 format.

```
<Sysname> system-view
[Sysname] public-key local export rsa name rsa1 ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-2011/05/12"
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDevEbyF93xHUJucJWqRc1r8fhzQ9lSVprCI6ATZeDYyR1J00fBQ8XY+
q2olqoagn5YDyUC8ZJvUhlyMOHeORpkAVxD3XncTp4XG66h3rTHHa7Xmm7f1GDYlF0n05t8mCLVaupbfCzP8b
a8UkrUmMO4fUvW6zavA5LYxtlAiQv0KQ==
---- END SSH2 PUBLIC KEY ----
```

Display the host public key of the local RSA key pair **rsa1** in OpenSSH format.

```
<Sysname> system-view
[Sysname] public-key local export rsa name rsa1 openssh
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDevEbyF93xHUJucJWqRc1r8fhzQ9lSVprCI6ATZeDYyR1J00fBQ8XY+
q2olqoagn5YDyUC8ZJvUhlyMOHeORpkAVxD3XncTp4XG66h3rTHHa7Xmm7f1GDYlF0n05t8mCLVaupbfCzP8b
a8UkrUmMO4fUvW6zavA5LYxtlAiQv0KQ== rsa-key
```

Related commands

`public-key local create`

`public-key peer import sshkey`

public-key peer

Use **`public-key peer`** to assign a name to a peer host public key and enter public key view, or enter the view of an existing peer host public key.

Use **`undo public-key peer`** to delete a peer host public key.

Syntax

public-key peer *keyname*

undo public-key peer *keyname*

Default

No peer host public keys exist.

Views

System view

Predefined user roles

network-admin

Parameters

keyname: Specifies a key name, a case-sensitive string of 1 to 64 characters.

Usage guidelines

After you execute this command to enter the public key view, type the public key. Spaces and carriage returns are allowed, but are not saved.

To configure a peer host public key on the local device, first obtain the peer public key in hexadecimal notation, and then perform the following tasks on the local device:

1. Execute the **public-key peer** command to enter public key view.
2. Type the public key.
3. Execute the **peer-public-key end** command to save the public key and return to system view.

The public key you type in the public key view must be in a correct format. If the peer device is an H3C device, use the **display public-key local public** command to display and record its public key.

Examples

Assign the name **key1** to the peer host public key and enter public key view.

```
<Sysname> system-view
[Sysname] public-key peer key1
Enter public key view. Return to system view with "peer-public-key end" command.
[Sysname-pkey-public-key-key1]
```

Related commands

display public-key local public

display public-key peer

peer-public-key end

public-key peer import sshkey

Use **public-key peer import sshkey** to import a peer host public key from a public key file.

Use **undo public-key peer** to remove a peer host public key.

Syntax

public-key peer *keyname* **import sshkey** *filename*

undo public-key peer *keyname*

Default

No peer host public keys exist.

Views

System view

Predefined user roles

network-admin

Parameters

keyname: Specifies a name for a peer host public key, a case-sensitive string of 1 to 64 characters.

filename: Specifies a public key file by its name, a case-insensitive string of 1 to 128 characters. The name cannot be all dots (.), hostkey, serverkey, dsakey, or ecdsakey, and cannot start with a slash (/) or contain ***./*** and ***../***. For more information about file names, see *Fundamentals Configuration Guide*.

Usage guidelines

After you configure this command, the system automatically transforms the host public key to the PKCS format, and saves the key.

Before you use this command, make sure you have got a copy of the public key file from the peer device through FTP in binary mode or through TFTP.

In non-FIPS mode, the device supports importing public keys in the format of SSH 1.5, SSH 2.0, and OpenSSH.

In FIPS mode, the device supports importing public keys in the format of SSH 2.0 and OpenSSH.

Examples

Import the peer host public key **key2** from the public key file **key.pub**.

```
<Sysname> system-view
[Sysname] public-key peer key2 import sshkey key.pub
```

Related commands

display public-key peer

public-key local export dsa

public-key local export ecdsa

public-key local export rsa

Contents

PKI commands

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

attribute

Use **attribute** to configure a rule to filter certificates based on an attribute in the certificate issuer name, subject name, or alternative subject name field.

Use **undo attribute** to remove an attribute rule.

Syntax

attribute *id* { **alt-subject-name** { **fqdn** | **ip** } | { **issuer-name** | **subject-name** } { **dn** | **fqdn** | **ip** } } { **ctn** | **equ** | **nctn** | **nequ** } *attribute-value*

undo attribute *id*

Default

No attribute rules exist.

Views

Certificate attribute group view

Predefined user roles

network-admin

Parameters

id: Specifies a rule ID in the range of 1 to 16.

alt-subject-name: Specifies the alternative subject name field.

fqdn: Specifies the FQDN attribute.

ip: Specifies the IP address attribute.

dn: Specifies the DN attribute.

issuer-name: Specifies the issuer name field.

subject-name: Specifies the subject name field.

ctn: Specifies the contain operation.

equ: Specifies the equal operation.

nctn: Specifies the not-contain operation.

nequ: Specifies the not-equal operation.

attribute-value: Sets an attribute value, a case-insensitive string of 1 to 128 characters.

Usage guidelines

Different certificate fields support different attributes.

- The subject name field and the issuer name field can contain a single DN, multiple FQDNs, and multiple IP addresses.
- The alternative subject name field can contain multiple FQDNs and IP addresses but zero DNs.

An attribute rule is a combination of an attribute-value pair with an operation keyword, as listed in Table 1.

Table 1 Combinations of attribute-value pairs and operation keywords

Operation	DN	FQDN/IP
ctn	The DN contains the specified attribute value.	Any FQDN or IP address contains the specified attribute value.
nctn	The DN does not contain the specified attribute value.	None of the FQDNs or IP addresses contain the specified attribute value.
equ	The DN is the same as the specified attribute value.	Any FQDN or IP address is the same as the specified attribute value.
nequ	The DN is not the same as the specified attribute value.	None of the FQDNs or IP addresses are the same as the specified attribute value.

A certificate matches an attribute rule if it contains an attribute that matches the criterion defined in the rule. For example, a certificate matches the **attribute 1 subject-name dn ctn abc** rule if it meets the following conditions:

- The subject name field of the certificate contains the DN attribute.
- The DN attribute value contains the **abc** string.

A certificate matches an attribute group if it matches all attribute rules in the group.

Examples

Create a certificate attribute group and enter its view.

```
<Sysname> system-view
[Sysname] pki certificate attribute-group mygroup
```

Configure an attribute rule to match certificates that contain the **abc** string in the subject DN.

```
[Sysname-pki-cert-attribute-group-mygroup] attribute 1 subject-name dn ctn abc
```

Configure an attribute rule to match certificates that do not contain FQDN **abc** in the issuer name field.

```
[Sysname-pki-cert-attribute-group-mygroup] attribute 2 issuer-name fqdn nequ abc
```

Configure an attribute rule to match certificates that do not contain IP address **10.0.0.1** in the alternative subject name field.

```
[Sysname-pki-cert-attribute-group-mygroup] attribute 3 alt-subject-name ip nequ 10.0.0.1
```

Related commands

display pki certificate attribute-group

rule

ca identifier

Use **ca identifier** to specify the trusted CA.

Use **undo ca identifier** to restore the default.

Syntax

ca identifier *name*

undo ca identifier

Default

No trusted CA is specified.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

name: Specifies the trusted CA by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

To obtain a CA certificate in a PKI domain, you must specify the trusted CA name. The trusted CA name uniquely identifies the CA to be used if multiple CAs exist on the CA server specified for the PKI domain.

Make sure the specified CA name is consistent with the name of the CA that owns the CA certificate to be obtained.

Examples

Set the name of the trusted CA to **new-ca**.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] ca identifier new-ca
```

certificate request entity

Use **certificate request entity** to specify the PKI entity for certificate request.

Use **undo certificate request entity** to restore the default.

Syntax

certificate request entity *entity-name*

undo certificate request entity

Default

No PKI entity is specified for certificate request.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

entity-name: Specifies a PKI entity by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

A PKI entity describes the identity attributes of an entity for certificate request, including the following information:

- Common name.
- Organization.
- Unit in the organization.
- Locality.
- State and country where the entity resides.
- FQDN.

- IP address.

You can specify only one PKI entity for a PKI domain. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify PKI entity **en1** for certificate request in PKI domain **aaa**.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] certificate request entity en1
```

Related commands

pki entity

certificate request from

Use **certificate request from** to specify the type of certificate request reception authority.

Use **undo certificate request from** to restore the default.

Syntax

certificate request from { **ca** | **ra** }

undo certificate request from

Default

The type of certificate request reception authority is not specified.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

ca: Sends certificate requests to the CA.

ra: Sends certificate requests to the RA.

Usage guidelines

The CA server determines whether the CA or RA accepts certificate requests. This authority setting must be consistent with the setting on the CA server.

Examples

Sends certificate requests to the RA.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] certificate request from ra
```

certificate request mode

Use **certificate request mode** to set the certificate request mode.

Use **undo certificate request mode** to restore the default.

Syntax

certificate request mode { **auto** [**password** { **cipher** | **simple** } *string*] | **manual** }

undo certificate request mode

Default

The certificate request mode is manual.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

auto: Specifies the auto certificate request mode.

password: Specifies a password for certificate revocation.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 31 characters. Its encrypted form is a case-sensitive string of 1 to 73 characters.

manual: Specifies the manual certificate request mode.

Usage guidelines

A certificate request can be submitted to a CA in offline or online mode. In online mode, a certificate request can be automatically or manually submitted:

- **Auto request mode**—A PKI entity automatically obtains the CA certificate and submits a certificate request to the CA when both of the following conditions exist:
  - An associated application (IKE, for example) performs identity authentication.
  - No certificate is available for the application on the device.

  In auto request mode, specify the password for certificate revocation as required by the CA policy.
- **Manual request mode**—You must manually obtain the CA certificate and submit certificate requests.

Examples

Set the certificate request mode to **auto**.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] certificate request mode auto
```

Set the certificate request mode to **auto**, and set the certificate revocation password in plain text to **123456**.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] certificate request mode auto password simple 123456
```

Related commands

pki request-certificate

certificate request polling

Use **certificate request polling** to set the polling interval and the maximum number of attempts to query certificate request status.

Use **undo certificate request polling** to restore the defaults.

Syntax

certificate request polling { **count** *count* | **interval** *interval* }

undo certificate request polling { **count** | **interval** }

Default

The polling interval is 20 minutes, and the maximum number of attempts is 50.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

count *count*: Specifies the maximum number of query attempts. The value range is 1 to 100.

interval *interval*: Specifies a polling interval in minutes. The value range is 5 to 168.

Usage guidelines

After a PKI entity submits a certificate request, it might take the CA server a while to issue the certificate if the CA administrator must manually approve the certificate request. During this period, the PKI entity periodically queries the CA server for the certificate request status. The periodic query operation stops until the PKI entity obtains the certificate or the maximum number of query attempts is reached. If the maximum number of query attempts is reached, the certificate request fails.

If the CA server automatically approves certificate requests, the PKI entity can obtain the certificate immediately after it submits a certificate request. In this case, the PKI entity does not send queries to the CA server.

Examples

Set the polling interval to 15 minutes, and the maximum number of query attempts to 40.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] certificate request polling interval 15
[Sysname-pki-domain-aaa] certificate request polling count 40
```

Related commands

display pki certificate request-status

certificate request url

Use **certificate request url** to specify the URL of the certificate request reception authority (CA or RA) to which the device should send SCEP certificate requests.

Use **undo certificate request url** to restore the default.

Syntax

certificate request url *url-string*

undo certificate request url

Default

The URL of the certificate request reception authority is not specified.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

url-string: Specifies the URL of the certificate request reception authority, a case-sensitive string of 1 to 511 characters. The URL length is restricted by the CLI string limitation or the *url-string* parameter, whichever is smaller.

Usage guidelines

The certificate request URL contains the location of the certificate request reception authority server and the path of the application script on the server, in the format http://*server_location/cgi_script_location.*

Examples

Set the certificate request URL to **http://169.254.0.1/certsrv/mscep/mscep.dll**.

```
<Sysname> system-view
[Sysname] pki domain a
[Sysname-pki-domain-a] certificate request url
http://169.254.0.1/certsrv/mscep/mscep.dll
```

common-name

Use **common-name** to set the common name for a PKI entity.

Use **undo common-name** to restore the default.

Syntax

common-name *common-name-sting*

undo common-name

Default

No common name is set for a PKI entity.

Views

PKI entity view

Predefined user roles

network-admin

Parameters

common-name-sting: Specifies a common name, a case-sensitive string of 1 to 63 characters. No comma can be included. You can set the username of the PKI entity as the common name.

Examples

Set the common name to **test** for PKI entity **en**.

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] common-name test
```

country

Use **country** to set the country code of a PKI entity.

Use **undo country** to restore the default.

Syntax

country *country-code-string*

undo country

Default

No country code is set for a PKI entity.

Views

PKI entity view

Predefined user roles

network-admin

Parameters

country-code-string: Specifies a country code, a case-sensitive string of two characters. For example, CN is the country code for China.

Examples

Set the country code to **CN** for PKI entity **en**.

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] country CN
```

crl check enable

Use **crl check enable** to enable CRL checking.

Use **undo crl check enable** to disable CRL checking.

Syntax

crl check enable

undo crl check enable

Default

CRL checking is enabled.

Views

PKI domain view

Predefined user roles

network-admin

Usage guidelines

A CRL is a list of revoked certificates signed and published by a CA. Revoked certificates should no longer be trusted.

Enable CRL checking to ensure that the device only accepts certificates that have not been revoked by the issuing CA.

Examples

Disable CRL checking.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] undo crl check enable
```

Related commands

pki import

pki retrieve-certificate

pki validate-certificate

crl url

Use **crl url** to specify the URL of the CRL repository.

Use **undo crl url** to restore the default.

Syntax

crl url *url-string*

undo crl url

Default

The URL of the CRL repository is not specified.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

url-string: Specifies the URL of the CRL repository, a case-sensitive string of 1 to 511 characters. The URL format is ldap://*server_location* or http://*server_location*. The URL length is restricted by the CLI string limitation or the *url-string* parameter, whichever is smaller.

Usage guidelines

To use CRL checking, a CRL must be obtained from a CRL repository.

The device selects a CRL repository in the following order:

1. CRL repository specified in the PKI domain by using this command.
2. CRL repository in the certificate that is being verified.
3. CRL repository in the CA certificate or CRL repository in the upper-level CA certificate if the CA certificate is the certificate being verified.

After the previous selection process, if the CRL repository is not found, the device obtains the CRL through SCEP. In this scenario, the CA certificate and the local certificates must have been obtained.

If an LDAP URL is specified, the device must connect to the LDAP server to obtain the CRL. If the LDAP URL does not contain the address of the LDAP server, use the **ldap-server** command to configure the server address in the PKI domain.

Examples

Set the URL of the CRL repository to **http://169.254.0.30**.

```
<Sysname> system-view
```

```
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] crl url http://169.254.0.30
```

Related commands

ldap-server

pki retrieve-crl

display pki certificate access-control-policy

Use **display pki certificate access-control-policy** to display information about certificate-based access control policies.

Syntax

display pki certificate access-control-policy [*policy-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

policy-name: Specifies a certificate-based access control policy by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

If you do not specify a policy name, this command displays information about all certificate-based access control policies.

Examples

Display information about certificate-based access control policy **mypolicy**.

```
<Sysname> display pki certificate access-control-policy mypolicy
 Access control policy name: mypolicy
     Rule 1  deny    mygroup1
     Rule 2  permit  mygroup2
```

Display information about all certificate-based access control policies.

```
<Sysname> display pki certificate access-control-policy
 Total PKI certificate access control policies: 2
 Access control policy name: mypolicy1
     Rule 1  deny    mygroup1
     Rule 2  permit  mygroup2
 Access control policy name: mypolicy2
     Rule 1  deny    mygroup3
     Rule 2  permit  mygroup4
```

Table 2 Command output

Field	Description
Total PKI certificate access control policies	Total number of certificate-based access control policies.

Field	Description
permit	Permit certificates that match the attribute group in the access control rule.
deny	Deny certificates that match the attribute group in the access control rule.

Related commands

pki certificate access-control-policy

rule

display pki certificate attribute-group

Use **display pki certificate attribute-group** to display information about certificate attribute groups.

Syntax

display pki certificate attribute-group [*group-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group-name: Specifies a certificate attribute group by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

If you do not specify a certificate attribute group, this command displays information about all certificate attribute groups.

Examples

Display information about certificate attribute group **mygroup**.

```
<Sysname> display pki certificate attribute-group mygroup
 Attribute group name: mygroup
      Attribute  1 subject-name     dn    ctn   abc
      Attribute  2 issuer-name      fqdn  nctn  app
```

Display information about all certificate attribute groups.

```
<Sysname> display pki certificate attribute-group
 Total PKI certificate attribute groups: 2.
 Attribute group name: mygroup1
      Attribute  1 subject-name     dn    ctn   abc
      Attribute  2 issuer-name      fqdn  nctn  app
Attribute group name: mygroup2
      Attribute  1 subject-name     dn    ctn   def
      Attribute  2 issuer-name      fqdn  nctn  fqd
```

Table 3 Command output

Field	Description
Total PKI certificate attribute groups	Total number of certificate attribute groups.
ctn	Contain operation.
nctn	Not-contain operation.
equ	Equal operation.
nequ	Not-equal operation.
Attribute 1 subject-name dn ctn abc	Attribute rule contents: • **alt-subject-name**—Alternative subject name. • **issuer-name**—Certificate issuer name. • **subject-name**—Certificate subject name. • **fqdn**—FQDN of the PKI entity. • **ip**—IP address of the PKI entity. • **dn**—DN of the PKI entity. • **ctn**—Indicates the contain operation. • **equ**—Indicates the equal operation. • **nctn**—Indicates the not-contain operation. • **nequ**—Indicates the not-equal operation.

Related commands

`attribute`

`pki certificate attribute-group`

display pki certificate domain

Use **`display pki certificate domain`** to display information about certificates.

Syntax

`display pki certificate domain` *`domain-name`* { **`ca`** | **`local`** | **`peer`** [**`serial`** *`serial-num`*] }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

`domain-name`: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in Table 4.

Table 4 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>

Character name	Symbol	Character name	Symbol
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

ca: Specifies the CA certificate.

local: Specifies the local certificates.

peer: Specifies the peer certificates.

serial *serial-num*: Specifies the serial number of a peer certificate.

Usage guidelines

If you specify the **CA** keyword, this command displays information about all CA certificates in the domain. If the domain has RA certificates, the RA certificates are also displayed.

If you specify the **local** keyword, this command displays information about all local certificates in the domain.

If you specify the **peer** keyword without a serial number, this command displays brief information about all peer certificates. If you specify a serial number, this command display detailed information about the specified peer certificate.

Examples

Display information about the CA certificate in PKI domain **aaa**.

```
<Sysname> display pki certificate domain aaa ca
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            5c:72:dc:c4:a5:43:cd:f9:32:b9:c1:90:8f:dd:50:f6
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=cn, O=docm, OU=rnd, CN=rootca
        Validity
            Not Before: Jan  6 02:51:41 2011 GMT
            Not After : Dec  7 03:12:05 2013 GMT
        Subject: C=cn, O=ccc, OU=ppp, CN=rootca
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:c4:fd:97:2c:51:36:df:4c:ea:e8:c8:70:66:f0:
                    28:98:ec:5a:ee:d7:35:af:86:c4:49:76:6e:dd:40:
                    4a:9e:8d:c0:cb:d9:10:9b:61:eb:0c:e0:22:ce:f6:
                    57:7c:bb:bb:1b:1d:b6:81:ad:90:77:3d:25:21:e6:
                    7e:11:0a:d8:1d:3c:8e:a4:17:1e:8c:38:da:97:f6:
                    6d:be:09:e3:5f:21:c5:a0:6f:27:4b:e3:fb:9f:cd:
                    c1:91:18:ff:16:ee:d8:cf:8c:e3:4c:a3:1b:08:5d:
                    84:7e:11:32:5f:1a:f8:35:25:c0:7e:10:bd:aa:0f:
                    52:db:7b:cd:5d:2b:66:5a:fb
                Exponent: 65537 (0x10001)
    Signature Algorithm: sha1WithRSAEncryption
        6d:b1:4e:d7:ef:bb:1d:67:53:67:d0:8f:7c:96:1d:2a:03:98:
```

```
        3b:48:41:08:a4:8f:a9:c1:98:e3:ac:7d:05:54:7c:34:d5:ee:
        09:5a:11:e3:c8:7a:ab:3b:27:d7:62:a7:bb:bc:7e:12:5e:9e:
        4c:1c:4a:9f:d7:89:ca:20:46:de:c5:b3:ce:36:ca:5e:6e:dc:
        e7:c6:fe:3f:c5:38:dd:d5:a3:36:ad:f4:3d:e6:32:7f:48:df:
        07:f0:a2:32:89:86:72:22:cd:ed:e5:0f:95:df:9c:75:71:e7:
        fe:34:c5:a0:64:1c:f0:5c:e4:8f:d3:00:bd:fa:90:b6:64:d8:
        88:a6
```

Display information about local certificates in the PKI domain **aaa**.

```
<Sysname> display pki certificate domain aaa local
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            bc:05:70:1f:0e:da:0d:10:16:1e
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=CN, O=sec, OU=software, CN=abdfdc
        Validity
            Not Before: Jan  7 20:05:44 2011 GMT
            Not After : Jan  7 20:05:44 2012 GMT
        Subject: O=OpenCA Labs, OU=Users, CN=fips fips-sec
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:b2:38:ad:8c:7d:78:38:37:88:ce:cc:97:17:39:
                    52:e1:99:b3:de:73:8b:ad:a8:04:f9:a1:f9:0d:67:
                    d8:95:e2:26:a4:0b:c2:8c:63:32:5d:38:3e:fd:b7:
                    4a:83:69:0e:3e:24:e4:ab:91:6c:56:51:88:93:9e:
                    12:a4:30:ad:ae:72:57:a7:ba:fb:bc:ac:20:8a:21:
                    46:ea:e8:93:55:f3:41:49:e9:9d:cc:ec:76:13:fd:
                    a5:8d:cb:5b:45:08:b7:d1:c5:b5:58:89:47:ce:12:
                    bd:5c:ce:b6:17:2f:e0:fc:c0:3e:b7:c4:99:31:5b:
                    8a:f0:ea:02:fd:2d:44:7a:67
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Cert Type:
                SSL Client, S/MIME
            X509v3 Key Usage:
                Digital Signature, Non Repudiation, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Client Authentication, E-mail Protection, Microsoft
Smartcardlogin
            Netscape Comment:
                User Certificate of OpenCA Labs
            X509v3 Subject Key Identifier:
                91:95:51:DD:BF:4F:55:FA:E4:C4:D0:10:C2:A1:C2:99:AF:A5:CB:30
```

```
            X509v3 Authority Key Identifier:
                keyid:DF:D2:C9:1A:06:1F:BC:61:54:39:FE:12:C4:22:64:EB:57:3B:11:9F

            X509v3 Subject Alternative Name:
                email:fips@ccc.com
            X509v3 Issuer Alternative Name:
                email:pki@openca.org
            Authority Information Access:
                CA Issuers - URI:http://titan/pki/pub/cacert/cacert.crt
                OCSP - URI:http://titan:2560/
                1.3.6.1.5.5.7.48.12 - URI:http://titan:830/

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://titan/pki/pub/crl/cacrl.crl

    Signature Algorithm: sha256WithRSAEncryption
        94:ef:56:70:48:66:be:8f:9d:bb:77:0f:c9:f4:65:77:e3:bd:
        ea:9a:b8:24:ae:a1:38:2d:f4:ab:e8:0e:93:c2:30:33:c8:ef:
        f5:e9:eb:9d:37:04:6f:99:bd:b2:c0:e9:eb:b1:19:7e:e3:cb:
        95:cd:6c:b8:47:e2:cf:18:8d:99:f4:11:74:b1:1b:86:92:98:
        af:a2:34:f7:1b:15:ee:ea:91:ed:51:17:d0:76:ec:22:4c:56:
        da:d6:d1:3c:f2:43:31:4f:1d:20:c8:c2:c3:4d:e5:92:29:ee:
        43:c6:d7:72:92:e8:13:87:38:9a:9c:cd:54:38:b2:ad:ba:aa:
        f9:a4:68:b5:2a:df:9a:31:2f:42:80:0c:0c:d9:6d:b3:ab:0f:
        dd:a0:2c:c0:aa:16:81:aa:d9:33:ca:01:75:94:92:44:05:1a:
        65:41:fa:1e:41:b5:8a:cc:2b:09:6e:67:70:c4:ed:b4:bc:28:
        04:50:a6:33:65:6d:49:3c:fc:a8:93:88:53:94:4c:af:23:64:
        cb:af:e3:02:d1:b6:59:5f:95:52:6d:00:00:a0:cb:75:cf:b4:
        50:c5:50:00:65:f4:7d:69:cc:2d:68:a4:13:5c:ef:75:aa:8f:
        3f:ca:fa:eb:4d:d5:5d:27:db:46:c7:f4:7d:3a:b2:fb:a7:c9:
        de:18:9d:c1
```

Display brief information about all peer certificates in the PKI domain **aaa**.

```
<Sysname> display pki certificate domain aaa peer
Total peer certificates: 1

Serial Number: 9a0337eb2156ba1f5476e4d754a5a9f7
Subject  Name: CN=sldsslserver
```

Display detailed information about a peer certificate in the PKI domain **aaa**.

```
<Sysname> display pki certificate domain aaa peer serial 9a0337eb2156ba1f5476e4d754a5a9f7

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            9a:03:37:eb:21:56:ba:1f:54:76:e4:d7:54:a5:a9:f7
        Signature Algorithm: sha1WithRSAEncryption
```

```
        Issuer: C=cn, O=ccc, OU=sec, CN=ssl
        Validity
            Not Before: Oct 15 01:23:06 2010 GMT
            Not After : Jul 26 06:30:54 2012 GMT
        Subject: CN=sldsslserver
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:c2:cf:37:76:93:29:5e:cd:0e:77:48:3a:4d:0f:
                    a6:28:a4:60:f8:31:56:28:7f:81:e3:17:47:78:98:
                    68:03:5b:72:f4:57:d3:bf:c5:30:32:0d:58:72:67:
                    04:06:61:08:3b:e9:ac:53:b9:e7:69:68:1a:23:f2:
                    97:4c:26:14:c2:b5:d9:34:8b:ee:c1:ef:af:1a:f4:
                    39:da:c5:ae:ab:56:95:b5:be:0e:c3:46:35:c1:52:
                    29:9c:b7:46:f2:27:80:2d:a4:65:9a:81:78:53:d4:
                    ca:d3:f5:f3:92:54:85:b3:ab:55:a5:03:96:2b:19:
                    8b:a3:4d:b2:17:08:8d:dd:81
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                keyid:9A:83:29:13:29:D9:62:83:CB:41:D4:75:2E:52:A1:66:38:3C:90:11

            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment,
Key Agreement
            Netscape Cert Type:
                SSL Server
            X509v3 Subject Alternative Name:
                DNS:docm.com
            X509v3 Subject Key Identifier:
                3C:76:95:9B:DD:C2:7F:5F:98:83:B7:C7:A0:F8:99:1E:4B:D7:2F:26
            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://s03130.ccc.sec.com:447/ssl.crl

    Signature Algorithm: sha1WithRSAEncryption
        61:2d:79:c7:49:16:e3:be:25:bb:8b:70:37:31:32:e5:d3:e3:
        31:2c:2d:c1:f9:bf:50:ad:35:4b:c1:90:8c:65:79:b6:5f:59:
        36:24:c7:14:63:44:17:1e:e4:cf:10:69:fc:93:e9:70:53:3c:
        85:aa:40:7e:b5:47:75:0f:f0:b2:da:b4:a5:50:dd:06:4a:d5:
        17:a5:ca:20:19:2c:e9:78:02:bd:19:77:da:07:1a:42:df:72:
        ad:07:7d:e5:16:d6:75:eb:6e:06:58:ee:76:31:63:db:96:a2:
        ad:83:b6:bb:ba:4b:79:59:9d:59:6c:77:59:5b:d9:07:33:a8:
        f0:a5
```

Related commands

pki domain

pki retrieve-certificate

display pki certificate request-status

Use **display pki certificate request-status** to display certificate request status.

Syntax

display pki certificate request-status [**domain** *domain-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in Table 5.

Table 5 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

Usage guidelines

If you do not specify a PKI domain, this command displays the certificate request status for all PKI domains.

Examples

Display certificate request status for PKI domain **aaa**.

```
<Sysname> display pki certificate request-status domain aaa
Certificate Request Transaction 1
    Domain name: aaa
    Status: Pending
    Key usage: General
    Remain polling attempts: 10
    Next polling attempt after : 1191 seconds
```

Display certificate request statuses for all PKI domains.

```
<Sysname> display pki certificate request-status
Certificate Request Transaction 1
    Domain name: domain1
    Status: Pending
    Key usage: General
    Remain polling attempts: 10
    Next polling attempt after : 1191 seconds
```

```
Certificate Request Transaction 2
    Domain name: domain2
    Status: Pending
    Key usage: Signature
    Remain polling attempts: 10
    Next polling attempt after : 188 seconds
```

Table 6 Command output

Field	Description
Certificate Request Transaction *number*	Certificate request transaction number, starting from 1.
Status	Certificate request status, including only the pending status.
Key usage	Certificate purposes: • **General**—Signature and encryption. • **Signature**—Signature only. • **Encryption**—Encryption only.
Remain polling attempts	Remaining number of attempts to query certificate request status.
Next polling attempt after	Remaining seconds before the next request status polling.

Related commands

`certificate request polling`

`pki domain`

`pki retrieve-certificate`

display pki crl domain

Use **`display pki crl domain`** to display information about the CRL saved at the local for a PKI domain.

Syntax

`display pki crl domain` *`domain-name`*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

`domain-name`: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in Table 7.

Table 7 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.

Character name	Symbol	Character name	Symbol
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

Usage guidelines

Use this command to determine whether a certificate has been revoked.

Examples

Display information about the CRL saved at the local for PKI domain **aaa**.

```
<Sysname> display pki crl domain aaa
Certificate Revocation List (CRL):
        Version 2 (0x1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: /C=cn/O=docm/OU=sec/CN=therootca
        Last Update: Apr 28 01:42:13 2011 GMT
        Next Update: NONE
        CRL extensions:
            X509v3 CRL Number:
                6
            X509v3 Authority Key Identifier:
                keyid:49:25:DB:07:3A:C4:8A:C2:B5:A0:64:A5:F1:54:93:69:14:51:11:EF

Revoked Certificates:
    Serial Number: CDE626BF7A44A727B25F9CD81475C004
        Revocation Date: Apr 28 01:37:52 2011 GMT
        CRL entry extensions:
            Invalidity Date:
                Apr 28 01:37:49 2011 GMT
    Serial Number: FCADFA81E1F56F43D3F2D3EF7EB56DE5
        Revocation Date: Apr 28 01:33:28 2011 GMT
        CRL entry extensions:
            Invalidity Date:
                Apr 28 01:33:09 2011 GMT
    Signature Algorithm: sha1WithRSAEncryption
        57:ac:00:3e:1e:e2:5f:59:62:04:05:9b:c7:61:58:2a:df:a4:
        5c:e5:c0:14:af:c8:e7:de:cf:2a:0a:31:7d:32:da:be:cd:6a:
        36:b5:83:e8:95:06:bd:b4:c0:36:fe:91:7c:77:d9:00:0f:9e:
        99:03:65:9e:0c:9c:16:22:ef:4a:40:ec:59:40:60:53:4a:fc:
        8e:47:57:23:e0:75:0a:a4:1c:0e:2f:3d:e0:b2:87:4d:61:8a:
        4a:cb:cb:37:af:51:bd:53:78:76:a1:16:3d:0b:89:01:91:61:
        52:d0:6f:5c:09:59:15:be:b8:68:65:0c:5d:1b:a1:f8:42:04:
        ba:aa
```

Table 8 Command output

Field	Description
Version	CRL version number.
Signature Algorithm	Signature algorithm used by the CA to sign the CRL.
Issuer	Name of the CA that issued the CRL.
Last Update	Most recent CRL update time.
Next Update	Next CRL update time.
X509v3 Authority Key Identifier	X509v3 ID of the CA that issues the CRL.
keyid	Key ID. This field identifies the key pair used to sign the CRL.
Signature Algorithm:	Signature algorithm and signature data.

Related commands

pki retrieve-crl

fqdn

Use **fqdn** to set the FQDN of an entity.

Use **undo fqdn** to restore the default.

Syntax

fqdn *fqdn-name-string*

undo fqdn

Default

No FQDN is set for a PKI entity.

Views

PKI entity view

Predefined user roles

network-admin

Parameters

fqdn-name-string: Specifies an FQDN, a case-sensitive string of 1 to 255 characters in the format *hostname*@*domainname*.

Usage guidelines

An FQDN uniquely identifies a PKI entity on a network.

Examples

Set the FQDN to **pki.domain-name.com** for PKI entity **en**.

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] fqdn abc@pki.domain.com
```

ip

Use **ip** to assign an IP address to a PKI entity.

Use **undo ip** to restore the default.

Syntax

ip { *ip-address* | **interface** *interface-type interface-number* }

undo ip

Default

No IP address is assigned to the PKI entity.

Views

PKI entity view

Predefined user roles

network-admin

Parameters

ip-address: Specifies an IPv4 address.

interface *interface-type interface-number*: Specifies an interface by its type and number. The primary IPv4 address of the interface will be used as the IP address of the PKI entity.

Usage guidelines

Use this command to assign an IP address to a PKI entity or specify an interface for the entity. The interface's primary IPv4 address will be used as the IP address of the PKI entity. If you specify an interface, make sure the interface is assigned an IP address before the PKI entity requests a certificate.

Examples

Assign IP address **192.168.0.2** to PKI entity **en**.

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] ip 192.168.0.2
```

ldap-server

Use **ldap-server** to specify an LDAP server for a PKI domain.

Use **undo ldap-server** to restore the default.

Syntax

ldap-server host *hostname* [**port** *port-number*]

undo ldap-server

Default

No LDAP server is specified for a PKI domain.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

host *hostname*: Specifies an LDAP server by its IPv4 address, IPv6 address, or domain name. The domain name is a case-sensitive string of 1 to 255 characters.

port *port-number*: Specifies the port number of the LDAP server. The value range is 1 to 65535, and the default is 389.

Usage guidelines

You must specify an LDAP server for a PKI domain in the following situations:

- The certificate repository uses LDAP for certificate distribution.
- The CRL repository uses LDAP for CRL distribution. However, the CRL repository URL configured for the PKI domain does not contain the IP address or host name of the LDAP server.

You can specify only one LDAP server for a PKI domain. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify LDAP server **10.0.0.1** for PKI domain **aaa**.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] ldap-server host 10.0.0.1
```

Related commands

pki retrieve-certificate

pki retrieve-crl

locality

Use **locality** to set the locality of a PKI entity.

Use **undo locality** to restore the default.

Syntax

locality *locality-name*

undo locality

Default

No locality is set for a PKI entity.

Views

PKI entity view

Predefined user roles

network-admin

Parameters

locality-name: Specifies a locality, a case-sensitive string of 1 to 63 characters. No comma can be included. You can set a city name as the locality.

Examples

Set the locality to **pukras** for PKI entity **en**.

```
<Sysname> system-view
[Sysname] pki entity en
```

```
[Sysname-pki-entity-en] locality pukras
```

organization

Use **organization** to set an organization name for a PKI entity.

Use **undo organization** to restore the default.

Syntax

organization *org-name*

undo organization

Default

No organization name is set for a PKI entity.

Views

PKI entity view

Predefined user roles

network-admin

Parameters

org-name: Specifies an organization name, a case-sensitive string of 1 to 63 characters. No comma can be included.

Examples

Set the organization name to **abc** for PKI entity **en**.

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] organization abc
```

organization-unit

Use **organization-unit** to set an organization unit name for a PKI entity.

Use **undo organization-unit** to restore the default.

Syntax

organization-unit *org-unit-name*

undo organization-unit

Default

No organization unit name is set for a PKI entity.

Views

PKI entity view

Predefined user roles

network-admin

Parameters

org-unit-name: Specifies an organization unit name, a case-sensitive string of 1 to 63 characters. No commas can be included.

Examples

Set the organization unit name to **rdtest** for PKI entity **en**.

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] organization-unit rdtest
```

pki abort-certificate-request

Use **pki abort-certificate-request** to abort the certificate request for a PKI domain.

Syntax

pki abort-certificate-request domain *domain-name*

Views

System view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in Table 9.

Table 9 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

Usage guidelines

You can abort a certificate request and change some parameters, such as common name, country code, or FQDN, in the certificate request before the CA issues the certificate. Use the **display pki certificate request-status** command to display the certificate request status.

Examples

Abort the certificate request for PKI domain **1**.

```
<Sysname> system-view
[Sysname] pki abort-certificate-request domain 1
The certificate request is in process.
Confirm to abort it? [Y/N]:y
```

Related commands

display pki certificate request-status

pki request-certificate domain

pki certificate access-control-policy

Use **pki certificate access-control-policy** to create a certificate-based access control policy and enter its view, or enter the view of an existing certificate-based access control policy.

Use **undo pki certificate access-control-policy** to remove a certificate-based access control policy.

Syntax

pki certificate access-control-policy *policy-name*

undo pki certificate access-control-policy *policy-name*

Default

No certificate-based access control policies exist.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a policy name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

A certificate-based access control policy contains a set of access control rules that permit or deny access to the device based on the attributes in the requesting client's certificate.

Examples

Create a certificate-based access control policy named **mypolicy** and enter its view.

```
<Sysname> system-view
[Sysname] pki certificate access-control-policy mypolicy
[Sysname-pki-cert-acp-mypolicy]
```

Related commands

display pki certificate access-control-policy

rule

pki certificate attribute-group

Use **pki certificate attribute-group** to create a certificate attribute group and enter its view, or enter the view of an existing certificate attribute group.

Use **undo pki certificate attribute-group** to remove a certificate attribute group.

Syntax

pki certificate attribute-group *group-name*

undo pki certificate attribute-group *group-name*

Default

No certificate attribute groups exist.

Views

System view

Predefined user roles

network-admin

Parameters

group-name: Specifies a group name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

A certificate attribute group is a set of attribute rules configured by using the **attribute** command. Each attribute rule defines a matching criterion for an attribute in the issuer name, subject name, or alternative subject name field of certificates.

A certificate attribute group must be associated with an access control rule (a permit or deny statement configured by using the **rule** command). If a certificate attribute group does not have any attribute rules, the system determines that the all certificates match the associated access control rule.

Examples

Create a certificate attribute group named **mygroup** and enter its view.

```
<Sysname> system-view
[Sysname] pki certificate attribute-group mygroup
[Sysname-pki-cert-attribute-group-mygroup]
```

Related commands

attribute

display pki certificate attribute-group

rule

pki delete-certificate

Use **pki delete-certificate** to remove certificates from a PKI domain.

Syntax

pki delete-certificate domain *domain-name* { **ca** | **local** | **peer** [**serial** *serial-num*] }

Views

System view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in Table 10.

Table 10 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"

Character name	Symbol	Character name	Symbol
Colon	:	Apostrophe	'

ca: Specifies the CA certificate.

local: Specifies the local certificates.

peer: Specifies the peer certificates.

serial *serial-num*: Specifies a peer certificate by its serial number, a case-insensitive string of 1 to 127 characters. If you do not specify a serial number, this command removes all peer certificates in the PKI domain.

Usage guidelines

When you remove the CA certificate in a PKI domain, the system also removes the local certificates, peer certificates, and the CRL in the PKI domain.

To delete a specific peer certificate in a PKI domain, perform the following steps:

1. Execute the **display pki certificate** command to determine the serial number of the peer certificate.
2. Execute the **pki delete-certificate domain** *domain-name* **peer serial** *serial-num* command.

Examples

Remove the CA certificate in PKI domain **aaa**.

```
<Sysname> system-view
[Sysname] pki delete-certificate domain aaa ca
Local certificates, peer certificates and CRL will also be deleted while deleting the CA certificate.
Confirm to delete the CA certificate? [Y/N]:y
[Sysname]
```

Remove the local certificates in PKI domain **aaa**.

```
<Sysname> system-view
[Sysname] pki delete-certificate domain aaa local
[Sysname]
```

Remove all peer certificates in PKI domain **aaa**.

```
<Sysname> system-view
[Sysname] pki delete-certificate domain aaa peer
[Sysname]
```

Display information about all peer certificates in PKI domain **aaa**, and remove a peer certificate with the specified serial number.

```
<Sysname> system-view
[Sysname] display pki certificate domain aaa peer
Total peer certificates: 1


Serial Number: 9a0337eb2156ba1f5476e4d754a5a9f7
Subject  Name: CN=abc
[Sysname] pki delete-certificate domain aaa peer serial 9a0337eb2156ba1f5476e4d754a5a9f7
```

Related commands

display pki certificate

pki domain

Use **pki domain** to create a PKI domain and enter its view, or enter the view of an existing PKI domain.

Use **undo pki domain** to remove a PKI domain.

Syntax

pki domain *domain-name*

undo pki domain *domain-name*

Default

No PKI domains exist.

Views

System view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a PKI domain name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in Table 11.

Table 11 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

Usage guidelines

When you remove a PKI domain, the certificates and the CRL in the domain are also removed.

Examples

Create a PKI domain named **aaa** and enter its view.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa]
```

pki entity

Use **pki entity** to create a PKI entity and enter its view, or enter the view of an existing PKI entity.

Use **undo pki entity** to remove a PKI entity.

Syntax

pki entity *entity-name*

undo pki entity *entity-name*

Default

No PKI entities exist.

Views

System view

Predefined user roles

network-admin

Parameters

entity-name: Specifies a name for a PKI entity, a case-insensitive string of 1 to 31 characters.

Usage guidelines

A PKI entity includes the identity information that can be used by a CA to identify a certificate applicant. You can configure multiple attributes for a PKI entity, such as common name, organization, organization unit, locality, state, country, FQDN, and IP address. The information will be included as subject contents in the certificate issued by the CA.

Examples

Create a PKI entity named **en** and enter its view.

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en]
```

Related commands

pki domain

pki export

Use **pki export** to export the CA certificate and the local certificates in a PKI domain.

Syntax

pki export domain *domain-name* **der** { **all** | **ca** | **local** } **filename** *filename*

pki export domain *domain-name* **p12** { **all** | **local** } **passphrase** *p12-key* **filename** *filename*

pki export domain *domain-name* **pem** { { **all** | **local** } [{ **3des-cbc** | **aes-128-cbc** | **aes-192-cbc** | **aes-256-cbc** | **des-cbc** } *pem-key*] | **ca** } [**filename** *filename*]

Views

System view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in Table 12.

Table 12 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.

Character name	Symbol	Character name	Symbol
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

der: Specifies the DER certificate file format, including PKCS#7.

p12: Specifies the PKCS#12 certificate file format.

pem: Specifies the PEM certificate file format.

all: Specifies both CA and local certificates. The RA certificate is excluded.

ca: Specifies the CA certificate.

local: Specifies the local certificates or the local certificates and their private keys.

passphrase *p12-key*: Specifies a password for encrypting the private key of a local PKCS12 certificate.

3des-cbc: Specifies 3DES_CBC for encrypting the private key of a local certificate.

aes-128-cbc: Specifies 128-bit AES_CBC for encrypting the private key of a local certificate.

aes-192-cbc: Specifies 192-bit AES_CBC for encrypting the private key of a local certificate.

aes-256-cbc: Specifies 256-bit AES_CBC for encrypting the private key of a local certificate.

des-cbc: Specifies DES_CBC for encrypting the private key of a local certificate.

pem-key: Specifies a password for encrypting the private key of a local certificate in PEM format.

filename *filename*: Specifies the name of the file for storing the certificate. The file name is a case-insensitive string. If you do not specify a file name when you export certificates in PEM format, this command displays the certificates on the terminal.

Usage guidelines

When you export the CA certificate, the following conditions might exist:

- If the PKI domain has only one CA certificate, this command exports the CA certificate to a file or displays it on the terminal.
- If the PKI domain has a CA certificate chain, this command exports the certificate chain to a file or displays it on the terminal.

When you export a local certificate to a local file, the local file name might be different from the file name specified in the command. The file name depends on the usage of the key pair contained in the certificate.

The following example uses **certificate** as the file name for saving an exported local certificate.

- If the local certificate contains an RSA signing key pair, the local file name is **certificate-signature**.
- If the local certificate contains an RSA encryption key pair, the local file name is **certificate-encryption**.
- If the local certificate contains a general purpose RSA, ECDSA, or DSA key pair, the local file name is **certificate**.

If the PKI domain has two local certificates, the local certificates are exported as follows:

- If you specify a file name, the two local certificates are exported to two different files.

- If you do not specify a file name, the local certificates are displayed on the terminal, separated by system prompts.

When you export all certificates, the following conditions might exist:

- If the PKI domain has only the CA certificate or local certificates, the result is the same as when you export the CA certificate or local certificates separately.
- If the PKI domain has both the CA certificate and local certificates, you get the following results:
  - If you specify a file name, each local certificate is exported to a separate file with their associated CA certificate chain.
  - If you do not specify a file name, the local certificates and CA certificate or CA certificate chain are displayed on the terminal, separated by system prompts.

When you export all certificates in PKCS12 format, the PKI domain must have a local certificate. If the domain does not have a local certificate, the export operation fails.

When you export the local certificates or all certificates in PEM format, you must specify the cryptographic algorithm and the challenge password for the private key. If you do not specify the cryptographic algorithm and the challenge password, this command does not export the private keys of the local certificates. If you specify the cryptographic algorithm and the password, and the local certificates have their private keys, this command can export the local certificates with their private keys. If the local certificates do not have their private keys, the export operation fails.

When you export the local certificates, if the key pair in the PKI domain is changed and no longer matches the key in the local certificates, the export operation fails.

When you export the local certificates or all certificates, if the PKI domain has two local certificates, failure of exporting one local certificate does not affect export of the other.

The specified file name can contain an absolute path. If the specified path does not exist, the export operation fails.

Examples

Export the CA certificate in the PKI domain to a file named **cert-ca.der** in DER format.

```
<Sysname> system-view
[Sysname] pki export domain domain1 der ca filename cert-ca.der
```

Export the local certificates in the PKI domain to a file named **cert-lo.der** in DER format.

```
<Sysname> system-view
[Sysname] pki export domain domain1 der local filename cert-lo.der
```

Export all certificates in the PKI domain to a file named **cert-all.p7b** in DER format.

```
<Sysname> system-view
[Sysname] pki export domain domain1 der all filename cert-all.p7b
```

Export the CA certificate in the PKI domain to a file named **cacert** in PEM format.

```
<Sysname> system-view
[Sysname] pki export domain domain1 pem ca filename cacert
```

Export the local certificates and their private keys in the PKI domain to a file named **local.pem** in PEM format. For the private keys, the cryptographic algorithm is DES_CBC and the password is 111.

```
<Sysname> system-view
[Sysname] pki export domain domain1 pem local des-cbc 111 filename local.pem
```

Export the all certificates in the PKI domain to a file named **all.pem** in PEM format. No cryptographic algorithm or password is specified, and the private keys are not exported.

```
<Sysname> system-view
[Sysname] pki export domain domain1 pem all filename all.pem
```

Display the local certificates and their private keys in the PKI domain on the terminal in PEM format. For the private keys, the cryptographic algorithm is DES_CBC and the password is 111.

```
<Sysname> system-view
[Sysname] pki export domain domain1 pem local des-cbc 111

%The signature usage local certificate:
Bag Attributes
    friendlyName:
    localKeyID: 99 0B C2 3B 8B D1 E4 33 42 2B 31 C3 37 C0 1D DF 0D 79 09 1D
subject=/C=CN/O=OpenCA Labs/OU=Users/CN=chktest chktest
issuer=/C=CN/O=OpenCA Labs/OU=software/CN=abcd
-----BEGIN CERTIFICATE-----
MIIEqjCCA5KgAwIBAgILAOhID4rI04kBfYgwDQYJKoZIhvcNAQELBQAwRTELMAkG
A1UEBhMCQ04xFDASBgNVBAoMC09wZW5DQSBMYWJzMREwDwYDVQQLDAhzb2Z0d2Fy
ZTENMAsGA1UEAwwEYWJjZDAeFw0xMTA0MjYxMzMxMjlaFw0xMjA0MjUxMzMxMjla
ME0xCzAJBgNVBAYTAkNOMRQwEgYDVQQKDAtPcGVuQ0EgTGFiczEOMAwGA1UECwwF
VXNlcnMxGDAWBgNVBAMMD2Noa3Rlc3QgY2hrdGVzdDCBnzANBgkqhkiG9w0BAQEF
AAOBjQAwgYkCgYEA54rUZ0Ux2kApceE4ATpQ437CU6ovuHS5eJKZyky8fhMoTHhE
jE2KfBQIzOZSgo2mdgpkccjr9Ek6IUC03ed1lPn0IG/YaAl4Tjgkiv+w1NrlSvAy
cnPaSUko2QbO9sg3ycye1zqpbbqj775ulGpcXyXYD9OY63/Cp5+DRQ92zGsCAwEA
AaOCAhUwggIRMAkGA1UdEwQCMAAwUAYDVR0gBEkwRzAGBgQqAwMEMAYGBCoDAwUw
NQYEKgMDBjAtMCsGCCsGAQUFBwIBFh9odHRwczovL3RpdGFuL3BraS9wdWIvY3Bz
L2Jhc2ljMBEGCWCGSAGG+EIBAQQEAwIFoDALBgNVHQ8EBAMCBsAwKQYDVR0lBCIw
IAYIKwYBBQUHAwIGCCsGAQUFBwMEBgorBgEEAYI3FAICMC4GCWCGSAGG+EIBDQQh
Fh9Vc2VyIENlcnRpZmljYXRlIG9mIE9wZW5DQSBMYWJzMB0GA1UdDgQWBBTPw8FY
ut7Xr2Ct/23zU/ybgU9dQjAfBgNVHSMEGDAWgBQzEQ58yIC54wxodp6JzZvn/gx0
CDAaBgNVHREEEzARgQ9jaGt0ZXN0QGgzYy5jb20wGQYDVR0SBBIwEIEOcGtpQG9w
ZW5jYS5vcmcwgYEGCCsGAQUFBwEBBHUwczAyBggrBgEFBQcwAoYmaHR0cDovL3Rp
dGFuL3BraS9wdWIvY2FjZXJ0L2NhY2VydC5jcnQwHgYIKwYBBQUHMAGGEmh0dHA6
Ly90aXRhbjoyNTYwLzAdBggrBgEFBQcwDIYRaHR0cDovL3RpdGFuOjgzMC8wPAYD
VR0fBDUwMzAxoC+gLYYraHR0cDovLzE5Mi4xNjguNDAuMTI4L3BraS9wdWIvY3Js
L2NhY3JsLmNybDANBgkqhkiG9w0BAQsFAAOCAQEAGcMeSpBJiuRmsJW0iZK5nygB
tgD8c0b+n4v/F36sJjY1fRFSr4gPLIxZhPWhTrqsCd+QMELRCDNHDxvt3/1NEG12
X6BVjLcKXKH/EQe0fnwK+7PegAJ15P56xDeACHz2oysvNQ0Ot6hGylMqaZ8pKUKv
UDS8c+HgIBrhmxvXztI08N1imYHq27Wy9j6NpSS60mMFmI5whzCWfTSHzqlT2DNd
no0id18SZidApfCZL8zoMWEFI163JZSarv+H5Kbb063dxXfbsqX9Noxggh0gD8dK
7X7/rTJuuhTWVof5gxSUJp+aCCdvSKg0lvJY+tJeXoaznrINVw3SuXJ+Ax8GEw==
-----END CERTIFICATE-----
Bag Attributes
    friendlyName:
    localKeyID: 99 0B C2 3B 8B D1 E4 33 42 2B 31 C3 37 C0 1D DF 0D 79 09 1D
Key Attributes: <No Attributes>
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIICwzA9BgkqhkiG9w0BBQ0wMDAbBgkqhkiG9w0BBQwwDgQIAbfcE+KoYYoCAggA
MBEGBSsOAwIHBAjB+UsJM07JRQSCAoABqtASbjGTQbdxL3n4wNHmyWLxbvL9v27C
Uu6MjYJDCipVzxHU0rExgn+6cQsK5uK99FPBmy4q9/nnyrooTX8BVlXAjenvgyii
WQLwnIg1IuM8j2aPkQ3wbae1+0RACjSLy1u/PCl5sp6CDxI0b9xz6cxIGxKvUOCc
/gxdgk97XZSW/0qnOSZkhgeqBZuxq6Va8iRyho7RCStVxQaeiAZpq/WoZbcS5CKI
/WXEBQd4AX2UxN0Ld/On7Wc6KFToixROTxWTtf8SEsKGPDfrEKq3fSTW1xokB8nM
bkRtU+fUiY27V/mr1RHO6+yEr+/wGGClBy5YDoD4I9xPkGUkmqx+kfYbMo4yxkSi


```

```
JdL+X3uEjHnQ/rvnPSKBEU/URwXHxMX9CdCTSqh/SajnrGuB/E4JhOEnS/H9dIM+
DN6iz1IwPFklbcK9KMGwV1bosymXmuEbYCYmSmhZb5FnR/RIyE804Jz9ifin3g0Q
ZrykfG7LHL7Ga4nh0hpEeEDiHGEMcQU+g0EtfpOLTI8cMJf7kdNWDnI0AYCvBAAM
3CY3BElDVjJq3ioyHSJca8C+3lzcueuAF+lO7Y4Zluq3dqWeuJjE+/1BZJbMmaQA
X6NmXKNzmtTPcMtojf+n3+uju0le0d0QYXQz/wPsV+9IYRYasjzoXE5dhZ5sIPOd
u9x9hhp5Ns23bwyNP135qTNjx9i/CZMKvLKywm3Yg+Bgg8Df4bBrFrsH1U0ifmmp
ir2+OuhlC+GbHOxWNeBCa8iAq91k6FGFJ0OLA2oIvhCnh45tM7BjjKTHk+RZdMiA
0TKSWuOyihrwxdUEWh999GKUpkwDHLZJFd21z/kWspqThodEx8ea
-----END ENCRYPTED PRIVATE KEY-----
```

Display all certificates in the PKI domain in PEM format. For the private keys, the cryptographic algorithm is DES_CBC and the password is 111.

```
<Sysname> system-view
[Sysname] pki export domain domain1 pem all des-cbc 111

 %The signature usage local certificate:
Bag Attributes
    friendlyName:
    localKeyID: 99 0B C2 3B 8B D1 E4 33 42 2B 31 C3 37 C0 1D DF 0D 79 09 1D
subject=/C=CN/O=OpenCA Labs/OU=Users/CN=chktest chktest
issuer=/C=CN/O=OpenCA Labs/OU=software/CN=abcd
-----BEGIN CERTIFICATE-----
MIIEqjCCA5KgAwIBAgILAOhID4rI04kBfYgwDQYJKoZIhvcNAQELBQAwRTELMAkG
A1UEBhMCQ04xFDASBgNVBAoMC09wZW5DQSBMYWJzMREwDwYDVQQLDAhzb2Z0d2Fy
ZTENMAsGA1UEAwwEYWJjZDAeFw0xMTA0MjYxMzMxMjlaFw0xMjA0MjUxMzMxMjla
ME0xCzAJBgNVBAYTAkNOMRQwEgYDVQQKDAtPcGVuQ0EgTGFiczEOMAwGA1UECwwF
VXNlcnMxGDAWBgNVBAMMD2Noa3Rlc3QgY2hrdGVzdDCBnzANBgkqhkiG9w0BAQEF
AAOBjQAwgYkCgYEA54rUZ0Ux2kApceE4ATpQ437CU6ovuHS5eJKZyky8fhMoTHhE
jE2KfBQIzOZSgo2mdgpkccjr9Ek6IUC03ed1lPn0IG/YaAl4Tjgkiv+w1NrlSvAy
cnPaSUko2QbO9sg3ycye1zqpbbqj775ulGpcXyXYD9OY63/Cp5+DRQ92zGsCAwEA
AaOCAhUwggIRMAkGA1UdEwQCMAAwUAYDVR0gBEkwRzAGBgQqAwMEMAYGBCoDAwUw
NQYEKgMDBjAtMCsGCCsGAQUFBwIBFh9odHRwczovL3RpdGFuL3BraS9wdWIvY3Bz
L2Jhc2ljMBEGCWCGSAGG+EIBAQQEAwIFoDALBgNVHQ8EBAMCBsAwKQYDVR0lBCIw
IAYIKwYBBQUHAwIGCCsGAQUFBwMEBgorBgEEAYI3FAICMC4GCWCGSAGG+EIBDQQh
Fh9Vc2VyIENlcnRpZmljYXRlIG9mIE9wZW5DQSBMYWJzMB0GA1UdDgQWBBTPw8FY
ut7Xr2Ct/23zU/ybgU9dQjAfBgNVHSMEGDAWgBQzEQ58yIC54wxodp6JzZvn/gx0
CDAaBgNVHREEEzARgQ9jaGt0ZXN0QGgzYy5jb20wGQYDVR0SBBIwEIEOcGtpQG9w
ZW5jYS5vcmcwgYEGCCsGAQUFBwEBBHUwczAyBggrBgEFBQcwAoYmaHR0cDovL3Rp
dGFuL3BraS9wdWIvY2FjZXJ0L2NhY2VydC5jcnQwHgYIKwYBBQUHMAGGEmh0dHA6
Ly90aXRhbjoyNTYwLzAdBggrBgEFBQcwDIYRaHR0cDovL3RpdGFuOjgzMC8wPAYD
VR0fBDUwMzAxoC+gLYYraHR0cDovLzE5Mi4xNjguNDAuMTI4L3BraS9wdWIvY3Js
L2NhY3JsLmNybDANBgkqhkiG9w0BAQsFAAOCAQEAGcMeSpBJiuRmsJW0iZK5nygB
tgD8c0b+n4v/F36sJjY1fRFSr4gPLIxZhPWhTrqsCd+QMELRCDNHDxvt3/1NEG12
X6BVjLcKXKH/EQe0fnwK+7PegAJ15P56xDeACHz2oysvNQ0Ot6hGylMqaZ8pKUKv
UDS8c+HgIBrhmxvXztI08N1imYHq27Wy9j6NpSS60mMFmI5whzCWfTSHzqlT2DNd
no0id18SZidApfCZL8zoMWEFI163JZSarv+H5Kbb063dxXfbsqX9Noxggh0gD8dK
7X7/rTJuuhTWVof5gxSUJp+aCCdvSKg0lvJY+tJeXoaznrINVw3SuXJ+Ax8GEw==
-----END CERTIFICATE-----
Bag Attributes: <No Attributes>
```

```
subject=/C=CN/O=OpenCA Labs/OU=software/CN=abcd
issuer=/C=CN/O=OpenCA Labs/OU=software/CN=abcd
-----BEGIN CERTIFICATE-----
MIIEYTCCA0mgAwIBAgIBFzANBgkqhkiG9w0BAQsFADBFMQswCQYDVQQGEwJDTjEU
MBIGA1UECgwLT3BlbkNBIExhYnMxETAPBgNVBAsMCHNvZnR3YXJlMQ0wCwYDVQQD
DARhYmNkMB4XDTExMDQxODExNDQ0N1oXDTEzMDQxNzExNDQ0N1owRTELMAkGA1UE
BhMCQ04xFDASBgNVBAoMC09wZW5DQSBMYWJzMREwDwYDVQQLDAhzb2Z0d2FyZTEN
MAsGA1UEAwwEYWJjZDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAM1g
vomMF8S4u6q51bOwjKFUBwxyvOy4D897LmOSedaCyDt6Lvp+PBEHfwWBYBpsHhk7
kmnSNhX5dZ6NxunHaARZ2VlcctsYKyvAQapuaThy1tuOcphAB+jQQL9dPoqdk0xp
jvmPDlW+k832Konn9U4dIivS0n+/KMGh0g5UyzHGqUUOo7s9qFuQf5EjQon40TZg
BwUnFYRlvGe7bSQpXjwi8LTyxHPy+dDVjO5CP+rXx5IiToFy1YGWewkyn/WeswDf
Yx7ZludNus5vKWTihgx2Qalgb+sqUMwI/WUET7ghO2dRxPUdUbgIYF0saTndKPYd
4oBgl6M0SMsHhe9nF5UCAwEAAaOCAVowggFWMA8GA1UdEwEB/wQFMAMBAf8wCwYD
VR0PBAQDAgEGMB0GA1UdDgQWBBQzEQ58yIC54wxodp6JzZvn/gx0CDAfBgNVHSME
GDAWgBQzEQ58yIC54wxodp6JzZvn/gx0CDAZBgNVHREEEjAQgQ5wa2lAb3BlbmNh
Lm9yZzAZBgNVHRIEEjAQgQ5wa2lAb3BlbmNhLm9yZzCBgQYIKwYBBQUHAQEEdTBz
MDIGCCsGAQUFBzAChiZodHRwOi8mdcGl0YW4vcGtpL3B1Yi9jYWNlcnQvY2FjZXJ0
LmNydDAeBggrBgEFBQcwAYYSaHR0cDovL3RpdGFuOjI1NjAvMB0GCCsGAQUFBzAM
hhFodHRwOi8mdcGl0YW46ODMwLzA8BgNVHR8ENTAzMDGgL6AthitodHRwOi8vMTky
LjE2OC40MC4xMjgvcGtpL3B1Yi9jcmwvY2FjcmwuY3JsMA0GCSqGSIb3DQEBCwUA
A4IBAQC0q0SSmvQNfa5ELtRKYF62C/Y8QTLbk6lZDTZuIzN15SGKQcbNM970ffCD
Lk1zosyEVE7PLnii3bZ5khcGO3byyXfluAqRyOGVJcudaw7uIQqgv0AJQ+zaQSHi
d4kQf5QWgYkQ55/C5puOmcMRgCbMpR2lYkqXLDjTIAZIHRZ/sTp6c+ie2bFxi/YT
3xYbO0wDMuGOKJJpsyKTKcbG9NdfbDyFgzEYAobyYqAUB3C0/bMfBduwhQWKSoYE
6vZsPGAEisCmAl3dIp49jPgVkixoShraYF1jLsWzJGlzem8QvWYzOqKEDwq3SV0Z
cXK8gzDBcsobcUMkwIYPAmd1kAPX
-----END CERTIFICATE-----
Bag Attributes
    friendlyName:
    localKeyID: 99 0B C2 3B 8B D1 E4 33 42 2B 31 C3 37 C0 1D DF 0D 79 09 1D
Key Attributes: <No Attributes>
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIICwzA9BgkqhkiG9w0BBQ0wMDAbBgkqhkiG9w0BBQwwDgQIcUSKSW9GVmICAggA
MBEGBSsOAwIHBAi5QZM+lSYWPASCAoBKDYulE5f2BXL9ZhI9zWAJpx2cShz/9PsW
5Qm106D+xSj1eAzkx/m4Xb4xRU8oOAuzu1DlWfSHKXoaa0OoRSiOEX1eg0eo/2vv
CHCvKHfTJr4gVSSa7i4I+aQ6AItrI6q99WlkN/e/IE5U1UE4ZhcsIiFJG+IvG7S8
f9liWQ2CImy/hjgFCD9nqSLN8wUzP7O2SdLVlUb5z4FR6VISZdgTFE8j7ko2HtUs
HVSg0nm114EwPtPMMbHefcuQ6b82y1M+dWfVxBN9K03lN4tZNfPWwLSRrPvjUzBG
dKtjf3/IFdV7/tUMy9JJSpt4iFt1h7SZPcOoGp1ZW+YUR30I7YnFE+9Yp/46KWT8
bk7j0STRnZX/xMy/9E52uHkLdW1ET3TXralLMYt/4jg4M0jUvoi3GS2Kbo+czsUn
gKgqwYnxVfRSvt8d6GBYrpF2tMFS9LEyngPKXExd+m4mAryuT5PhdFTkb1B190Lp
UIBjk3IXnr7AdrhvyLkH0UuQE95emXBD/K0HlD73cMrtmogL8F4yS5B2hpIr/v5/
eW35+1QMnJ9FtHFnVsLx9wl9lX8iNfsoBhg6FQ/hNSioN7rNBe7wwIRzxPVfEhO8
5ajQxWlidRn5RkzfUo6HuAcq02QTpSXI6wf2bzsVmr5sk+fRaELD/cwL6VjtXO6x
ZBLJcUyAwvScrOtTEK7Q5n0I34gQd4qcF0D1x9yQ4sqvTeU/7Jkm6XCPV05/5uiF
RLCfFAwaJMBdIQ6jDQHnpWT67uNDwdEzaPmuTVMme5Woc5zsqE5DY3hWu4oqFdDz
kPLnbX74IZ0gOLki9eIJkVswnF5HkBCKS50ejlW6TgbMNZ+JPk2w
```

```
-----END ENCRYPTED PRIVATE KEY-----
```

Display the CA certificate in the PKI domain in PEM format.

```
<Sysname> system-view
[Sysname]pki export domain domain1 pem ca
-----BEGIN CERTIFICATE-----
MIIB+TCCAWICEQDMbgjRKygg3vpGFVY6pa3ZMA0GCSqGSIb3DQEBBQUAMD0xCzAJ
BgNVBAYTAmNuMQwwCgYDVQQKEwNoM2MxETAPBgNVBAsTCGgzYy10ZXN0MQ0wCwYD
VQQDEwQ4MDQzMB4XDTExMDMyMjA0NDQyNFoXDTE0MDMyMzA0MzUyNFowPTELMAkG
A1UEBhMCY24xDDAKBgNVBAoTA2gzYzERMA8GA1UECxMIaDNjLXRlc3QxDTALBgNV
BAMTBDgwNDMwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAOvDAYQhyc++G7h5
eNDzJs22OQjCn/4JqnNKIdKz1BbaJT8/+IueSn9JIsg64Ex2WBeCd/tcmnSW57ag
dCvNIUYXXVOGca2iaSOElqCF4CQfV9zLrBtA7giHD49T+JbxLrrJLmdIQMJ+vYdC
sCxIp3YMAiuCahVLZeXklooqwqIXAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAElm7
W2Lp9Xk4nZVIpVV76CkNe8/C+Id00GCRUUVQFSMvo7Pded76bmYX2KzJSz+DlMqy
TdVrgG9Fp6XTFO80aKJGe6NapsfhJHKS+Q7mL0XpXeMONgK+e3dX7rsDxsY7hF+j
0gwsHrjV7kWvwJvDlhzGW6xbpr4DRmdcao19Cr6o=
-----END CERTIFICATE-----
```

Export the CA certificate in the PKI domain to a file named **cacert** in PEM format.

```
<Sysname> system-view
[Sysname] pki export domain domain1 pem ca filename cacert
```

Display the CA certificate or the CA certificate chain in the PKI domain on the terminal.

```
<Sysname> system-view
[Sysname]pki export domain domain1 pem ca
-----BEGIN CERTIFICATE-----
MIIB7jCCAVcCEQCdSVShJFEMifVG8zRRoSsWMA0GCSqGSIb3DQEBBQUAMDcxCzAJ
BgNVBAYTAmNuMQwwCgYDVQQKEwNoM2MxDDAKBgNVBAsTA2gzYzEMMAoGA1UEAxMD
YWNhMB4XDTExMDEwNjAyNTc0NFoXDTEzMTIwMTAzMTMyMFowODELMAkGA1UEBhMC
Y24xDDAKBgNVBAoTA2gzYzEMMAoGA1UECxMDaDNjMQ0wCwYDVQQDEwRhYWNhMIGf
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDcuJsWhAJXEDmowGb5z7VDVms54TKi
xnaNJCWvBOrU64ftvpVB7xQekbkjgAS9FjDyXlLQ8IyIsYIp5ebJr8P+n9i9Pl7j
lBx5mi4XeIldyv2OjfNx5oSQ+gWY9/m1R8uv13RS05r3rxPg+7EvKBjmiy0Giddw
vu3Y3WrjBPp6GQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAJrQddzVQEiy4AcgtzUL
ltkmlmWoz87+jUsgFB+H+xeyiZE4sancf2UwH8kXWqZ5AuReFCCBC2fkvvQvUGnV
cso7JXAhfw8sUFok9eHz2R+GSoEk5BZFzZ8eCmNyGq9ln6mJsO1hAqMpsCW6G2zh
5mus7FTHhywXpJ22/fnHg61m
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB8DCCAVkCEQD2PBUx/rvslNw9uTrZB3DlMA0GCSqGSIb3DQEBBQUAMDoxCzAJ
BgNVBAYTAmNuMQwwCgYDVQQKEwNoM2MxDDAKBgNVBAsTA2gzYzEPMA0GA1UEAxMG
cm9mdcGNhMB4XDTExMDEwNjAyNTY1OFoXDTEzMTIwNDAzMTMxMFowNzELMAkGA1UE
BhMCY24xDDAKBgNVBAoTA2gzYzEMMAoGA1UECxMDaDNjMQwwCgYDVQQDEwNhY2Ew
gZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAOeklR7DpeEV72N1OLz+dydIDTx0
zVZDdPxF1gQYWSfIBwwFKJEyQ/4y8VIfDIm0EGTM4dsOX/QFwudhl/Czkio3dWLh
Q1y5XCJy68vQKrB82WZ2mah5Nuekus3LSZZBoZKTAOY5MCCMFcULM858dtSq15Sh
xF7tKSeAT7ARlJxTAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEADJQCo6m0RNup0ewa
ItX4XK/tYcJXAQWMA0IuwaWpr+ofqVVgYBPwVpYglhJDOuIZxKdR2pfQOA4f35wM
Vz6kAujLATsEA1GW9ACUWa5PHwVgJk9BDEXhKSJ2e7odmrg/iROhJjc1NMV3pvIs
CuFiCLxRQcMGhCNHlOn4wuydssc=
```

```
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB8jCCAVsCEFxy3MSlQ835MrnBkI/dUPYwDQYJKoZIhvcNAQEFBQAwOjELMAkG
A1UEBhMCY24xDDAKBgNVBAoTA2gzYzEMMAoGA1UECxMDaDNjMQ8wDQYDVQQDEwZy
b290Y2EwHhcNMTEwMTA2MDI1MTQxWhcNMTMxMjA3MDMxMjA1WjA6MQswCQYDVQQG
EwJjbjEMMAoGA1UEChMDaDNjMQwwCgYDVQQLEwNoM2MxDzANBgNVBAMTBnJvb3Rj
YTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAxP2XLFE230zq6MhwZvAomOxa
7tc1r4bESXZu3UBKno3Ay9kQm2HrDOAizvZXfLu7Gx22ga2Qdz0lIeZ+EQrYHTyO
pBcejDjal/ZtvgnjXyHFoG8nS+P7n83BkRj/Fu7Yz4zjTKMbCF2EfhEyXxr4NSXA
fhC9qg9S23vNXStmWvsCAwEAATANBgkqhkiG9w0BAQUFAAOBgQBtsU7X77sdZ1Nn
0I98lh0qA5g7SEEIpI+pwZjjrH0FVHw01e4JWhHjyHqrOyfXYqe7vH4SXp5MHEqf
14nKIEbexbPONspebtznxv4/xTjd1aM2rfQ95jJ/SN8H8KIyiYZyIs3t5Q+V35x1
cef+NMWgZBzwXOSP0wC9+pC2ZNiIpg==
-----END CERTIFICATE-----
```

Export the local certificates and their private keys in the PKI domain to a file named **cert-lo.der** in PKCS12 format. The password for the private keys is 123.

```
<Sysname> system-view
[Sysname] pki export domain domain1 p12 local passphrase 123 filename cert-lo.der
```

Export all certificates in the PKI domain to a file named **cert-all.p7b** in PKCS12 format.

```
<Sysname> system-view
[Sysname] pki export domain domain1 p12 all passphrase 123 filename cert-all.p7b
```

Related commands

pki domain

pki import

Use **pki import** to import the CA certificate, local certificates, or peer certificates for a PKI domain.

Syntax

pki import domain *domain-name* { **der** { **ca** | **local** | **peer** } **filename** *filename* | **p12 local filename** *filename* | **pem** { **ca** | **local** | **peer** } [**filename** *filename*] }

Views

System view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in Table 13.

Table 13 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"

Character name	Symbol	Character name	Symbol
Colon	:	Apostrophe	'

der: Specifies the DER certificate file format, including PKCS#7.

p12: Specifies the PKCS#12 certificate file format.

pem: Specifies the PEM certificate file format.

ca: Specifies the CA certificate.

local: Specifies the local certificates.

peer: Specifies the peer certificates.

filename *filename*: Specifies a certificate file name, a case-insensitive string. For a certificate in PEM format, you can also choose to copy and paste the certificate contents on the terminal instead of importing from a file.

Usage guidelines

Use this command to import a certificate in the following situations:

- The CRL repository is not specified or the CA server does not support SCEP.
- The certificate is packed with the server generated key pair in a single file. Only certificate files in PKCS12 or PEM format can contain key pairs.

Before you import certificates, complete the following tasks:

- Use FTP or TFTP to upload the certificate files to the storage media of the device. If FTP or TFTP is not available, display and copy the contents of a certificate to a file on the device. Make sure the certificate is in PEM format because only certificates in PEM format can be imported by this means.
- For the local certificates or peer certificates to be imported, the correct CA certificate chain must exist. The CA certificate chain can be stored on the device, or carried in the local certificates or peer certificates. If the PKI domain, the local certificates, or the peer certificates do not have the CA certificate chain, you must import the CA certificate first. To import a local or peer certificate, a CA certificate chain must exist in the PKI domain, or be carried in the local or peer certificate. If not, obtain it first.

When you import the local or peer certificates:

- If the local or peer certificates contain the CA certificate chain, you can import the CA certificate and the local or peer certificates at the same time. If the CA certificate already exists in a PKI domain, the system prompts you whether to overwrite the existing CA certificate.
- If the local or peer certificates do not contain the CA certificate chain, but the CA certificate already exists in a PKI domain, you can directly import the certificates.

You can import the CA certificate to a PKI domain when either of the following conditions is met:

- The CA certificate to be imported is the root CA certificate or contains the certificate chain with the root certificate.
- The CA certificate contains a certificate chain without the root certificate, but can form a complete certificate chain with an existing CA certificate on the device.

Contact the CA administrator to get information as prompted in the following scenarios:

- The system prompts you to confirm the certificate's fingerprint in the following situation:
  - The certificate file to be imported contains the root certificate, but the root certificate does not exist in any PKI domains on the device.
  - The **root-certificate fingerprint** command is not configured in the PKI domain to which the certificate file is to be imported.

- The system prompts you to enter the challenge password used for encrypting the private key if the local certificate to be imported contains a key pair.

When you import a local certificate file that contains a key pair, you can choose to update the domain with the key pair. Depending on the purpose of the key pair, the following conditions might apply:

- If the purpose of the key pair is general, the device uses the key pair to replace the local key pair that is found in this order:
  a. General-purpose key pair.
  b. Signature key pair.
  c. Encryption key pair.
- If the purpose of the key pair is signature, the device uses the key pair to replace the local key pair that is found in this order:
  a. General-purpose key pair.
  b. Signature key pair.
- If the purpose of the key pair is encryption, the device searches the domain for an encryption key pair.

If a matching key pair is found, the device asks whether you want to overwrite the existing key pair on the device. If no match is found, the device asks you to enter a key pair name (defaulting to the PKI domain name). Then, it generates the key pair according to the key algorithm and the purpose defined in the certificate file.

The import operation automatically updates or generates the correct key pair. When you perform the import operation, be sure to save the configuration file to avoid data loss.

Examples

Import CA certificate file **rootca_pem.cer** in PEM format to PKI domain **aaa**. The certificate file contains the root certificate.

```
<Sysname> system-view
[Sysname] pki import domain aaa pem ca filename rootca_pem.cer
The trusted CA's finger print is:
    MD5  fingerprint:FFFF 3EFF FFFF 37FF FFFF 137B FFFF 7535
    SHA1 fingerprint:FFFF FF7F FF2B FFFF 7618 FF4C FFFF 0A7D FFFF FF69
Is the finger print correct?(Y/N):y
[Sysname]
```

Import CA certificate file **aca_pem.cer** in PEM format to PKI domain **bbb**. The certificate file does not contain the root certificate.

```
<Sysname> system-view
[Sysname] pki import domain bbb pem ca filename aca_pem.cer
[Sysname]
```

Import local certificate file **local-ca.p12** in PKCS12 format to PKI domain **bbb**. The certificate file contains a key pair.

```
<Sysname> system-view
[Sysname] pki import domain bbb p12 local filename local-ca.p12
Please input challenge password:
******
[Sysname]
```

Import the local certificate in PEM format to PKI domain **bbb** by copying and pasting the contents of the certificate. The certificate contains the key pair and the CA certificate chain.

```
<Sysname> system-view
[Sysname] pki import domain bbb pem local
Enter PEM-formatted certificate.
```

```
End with a Ctrl+c on a line by itself.
Bag Attributes
localKeyID: 01 00 00 00
friendlyName: {F7619D96-3AC2-40D4-B6F3-4EAB73DEED73}
Microsoft CSP Name: Microsoft Enhanced Cryptographic Provider v1.0
Key Attributes
X509v3 Key Usage: 10
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,8DCE37F0A61A4B8C

k9C3KHY5S3EtnF5iQymvHYYrVFy5ZdjSasU5y4XFubjdcvmpFHQteMjD0GKX6+xO
kuKbvpyCnWsPVg56sL/PDRyrRmqLmtUV3bpyQsFXgnc7p+Snj3CG2Ciow9XApybW
Ec1TDCD75yuQckpVQdhguTvoPQXf9zHmiGu5jLkySp2k7ec/Mc97Ef+qqpfnHpQp
GDmMqnFpp59ZzB21OGlbGzlPcsjoT+EGpZg6B1KrPiCyFim95L9dWVwX9sk+U1s2
+8wqac8jETwwM0UZ1NGJ50JJz1QYIzMbcrw+S5WlPxACTIz1cldlBlb1kpc+7mcX
4W+MxFzsL88IJ99T72eu4iUNsy26g0BZMAcc1sJA3A4w9RNhfs9hSG43S3hAh5li
JPp720LfYBlkQHn/MgMCZASWDJ5G0eSXQt9QymHAth4BiT9v7zetnQqf4q8plfd/
Xqd9zEFlBPpoJFtJqXwxHUCKgw6kJeC4CxHvi9ZCJU/upg9IpiguFPoaDOPia+Pm
GbRqSyy55clVde5GOccGN1DZ94DW7AypazgLpBbrkIYAdjFPRmq+zMOdyqsGMTNj
jnheI5l784pNOAKuGi0i/uXmRRcfoMh6qAnK6YZGS7rOLC9CfPmy8fgY+/Sl9d9x
Q00ruO1psxzh9c2YfuaiXFIx0auKl6o5+ZZYn7Rg/xy2Y0awVP+dO925GoAcHO40
cCl6jA/HsGAU9HkpwKHL35lmBDRLEzQeBFcaGwSm1JvRfE4tkJM7+Uz2QHJOfP10
0VLqMgxMlpk3TvBWgzHGJDe7TdzFCDPMPhod8pi4P8gGXmQd01PbyQ==
-----END RSA PRIVATE KEY-----
Bag Attributes
localKeyID: 01 00 00 00
subject=/CN=sldsslserver
issuer=/C=cn/O=ccc/OU=sec/CN=ssl
-----BEGIN CERTIFICATE-----
MIICjzCCAfigAwIBAgIRAJoDN+shVrofVHbk11SlqfcwDQYJKoZIhvcNAQEFBQAw
NzELMAkGA1UEBhMCY24xDDAKBgNVBAoTA2gzYzEMMAoGA1UECxMDc2VjMQwwCgYD
VQQDEwNzc2wwHhcNMTAxMDE1MDEyMzA2WhcNMTIwNzI2MDYzMDU0WjAXMRUwEwYD
VQQDEwxzbGRzc2xzZXJ2ZXIwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMLP
N3aTKV7NDndIOk0PpiikYPgxVih/geMXR3iYaANbcvRX07/FMDINWHJnBAZhCDvp
rFO552loGiPyl0wmFMK12TSL7sHvrxr0OdrFrqtWlbW+DsNGNcFSKZy3RvIngC2k
ZZqBeFPUytP185JUhbOrVaUDlisZi6NNshcIjd2BAgMBAAGjgbowgbcwHwYDVR0j
BBgwFoAUmoMpEynZYoPLQdR1LlKhZjg8kBEwDgYDVR0PAQH/BAQDAgP4MBEGCWCG
SAGG+EIBAQQEAwIGQDASBgNVHREECzAJggdoM2MuY29tMB0GA1UdDgQWBBQ8dpWb
3cJ/X5iDt8eg+JkeS9cvJjA+BgNVHR8ENzA1MDOgMaAvhi1odHRwOi8vczAzMTMw
LmgzYy5odWF3ZWktM2NvbS5jb206NDQ3L3NzbC5jcmwwDQYJKoZIhvcNAQEFBQAD
gYEAYS15x0kW474lu4twNzEy5dPjMSwtwfm/UK01S8GQjGV5tl9ZNiTHFGNEFx7k
zxBp/JPpcFM8hapAfrVHdQ/wstq0pVDdBkrVF6XKIBks6XgCvRl32gcaQt9yrQd9
5RbWdetuBljudjFj25airYO2u7pLeVmdWWx3WVvZBzOo8KU=
-----END CERTIFICATE-----
Bag Attributes: <Empty Attributes>
subject=/C=cn/O=ccc/OU=sec/CN=ssl
issuer=/C=cn/O=ccc/OU=sec/CN=ssl
```

```
-----BEGIN CERTIFICATE-----
MIIB7DCCAVUCEG+jJTPxxiE67pl2ff0SnOMwDQYJKoZIhvcNAQEFBQAwNzELMAkG
A1UEBhMCY24xDDAKBgNVBAoTA2gzYzEMMAoGA1UECxMDc2VjMQwwCgYDVQQDEwNz
c2wwHhcNMDkwNzMxMDY0ODQ2WhcNMTIwNzI5MDYyODU4WjA3MQswCQYDVQQGEwJj
bjEMMAoGA1UEChMDaDNjMQwwCgYDVQQLEwNzZWMxDDAKBgNVBAMTA3NzbDCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAt8QSMetQ70GONiFh7iJkvGQ8nC15zCF1
cqC/RcJhE/88LkKyQcu9j+Tz8Bk9Qj2UPaZdrk8fOrgtBsa7lZ+UO3j3l30q84l+
HjWq8yxVLRQahU3gqJze6pGR2l0s76u6GRyCX/zizGrHKqYlNnxK44NyRZx2klQ2
tKQAfpXCPIkCAwEAATANBgkqhkiG9w0BAQUFAAOBgQBWsaMgRbBMtYNrrYCMjY6g
c7PBjvajVOKNUMxaDalePmXfKCxl91+PKM7+i8I/zLcoQO+sHbva26a2/C4sNvoJ
2QZs6GtAOahP6CDqXC5VuNBU6eTKNKjL+mf6uuDeMxrlDNha0iymdrXXVIp5cuIu
fl7xgArs8Ks6aXDXM1o4DQ==
-----END CERTIFICATE-----


Please input the password:********
Local certificate already exist, confirm to overwrite it? [Y/N]:y
The PKI domain already has a CA certificate. If it is overwritten, local certificates, peer certificates and CRL of this domain will also be deleted.
Overwrite it? [Y/N]:y
The system is going to save the key pair. You must specify a key pair name, which is a case-insensitive string of 1 to 64 characters. Valid characters include a to z, A to Z, 0 to 9, and hyphens (-).
Please enter the key pair name [default name: bbb]:

The key pair already exists.
Please enter the key pair name:
import-key
```

Related commands

display pki certificate

public-key dsa

public-key ecdsa

public-key rsa

pki request-certificate

Use **pki request-certificate** to submit a local certificate request or generate a certificate request in PKCS#10 format.

Syntax

pki request-certificate domain *domain-name* [**password** *password*] [**pkcs10** [**filename** *filename*]]

Views

System view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in Table 14.

Table 14 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

password *password*: Sets the password for certificate revocation, a case-sensitive string of 1 to 31 characters. The password is contained in the certificate request and must be provided if the certificate is revoked.

pkcs10: Displays BASE64-encoded PKCS#10 certificate request information, which can be used to request a certificate by an out-of-band means, like phone, disk, or email.

filename *filename*: Specifies a local file for saving the certificate request in PKCS#10 format. The *filename* argument is case-insensitive.

Usage guidelines

If SCEP fails, you can perform one of the following tasks:

- Use the **pkcs10** keyword to print the BASE64-encoded request information.
- Use the **pkcs10 filename** *filename* option to save the request information to a local file and transfer the file to the CA by using an out-of-band means. The file name can contain an absolute path. If the specified path does exist, the request information cannot be saved.

This command is not saved in the configuration file.

Examples

Display information about the certificate request in PKCS#10 format.

```
<Sysname> system-view
[Sysname] pki request-certificate domain aaa pkcs10

*** Request for general certificate ***
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBTDCBtgIBADANMQswCQYDVQQDEwJqajCBnzANBgkqhkiG9w0BAQEFAAOBjQAw
gYkCgYEAw5Drj8ofs9THA4ezkDcQPBy8pvH1kumampPsJmx8sGG52NFtbrDTnTT5
ALx3LJijB3d/ndKpcHT/DfbJVDCn5gdw32tBZyCkEwMHZN3ol2z7Nmdcu5TED6iN8
4m+hfp1QWoV6lty3o9pxAXuQl8peUDcfN6WV3LBXYyl1WCtkLkECAwEAAaAAMA0G
CSqGSIb3DQEBBAUAA4GBAA8E7BaIdmT6NVCZgv/I/1tqZH3TS4e4H9Qo5NiCKiEw
R8owVmA0XVtGMbyqBNcDTG0f5NbHrXZQT5+MbFJOnm5K/mn1ro5TJKMTKV46PlCZ
JUjsugaY02GBY0BVcylpC9iIXLuXNIqjh1MBIqVsa1lQOHS7YMvnop6hXAQlkM4c
-----END NEW CERTIFICATE REQUEST-----
```

Request the local certificates.

```
[Sysname] pki request-certificate domain openca
Start to request general certificate ...
…
```

```
Request certificate of domain openca successfully
```

Related commands

display pki certificate

pki retrieve-certificate

Use **pki retrieve-certificate** to obtain a certificate from the certificate distribution server.

Syntax

pki retrieve-certificate domain *domain-name* { **ca** | **local** | **peer** *entity-name* }

Views

System view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in Table 15.

Table 15 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

ca: Specifies the CA certificate.

local: Specifies the local certificates.

peer *entity-name*: Specifies a peer entity by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

In online mode:

- You can obtain the CA certificate through the SCEP protocol. If a CA certificate already exists locally, do not obtain the CA certificate again. To obtain a new CA certificate, use the **pki delete-certificate** command to remove the CA certificate and local certificates, and then obtain the CA certificate again.
- You can obtain local certificates or peer certificates through the LDAP protocol. If a PKI domain already has local certificates or peer certificates, you can still perform the obtain operation and the obtained local certificates or peer certificates overwrite the existing ones. If RSA is used, a PKI domain can have two local certificates, one for signing and the other for encryption. Certificates for different purposes do not overwrite each other.

The obtained CA certificate, local certificates, and peer certificates are automatically verified before they are saved locally. If the verification fails, they are not saved.

This command is not saved in the configuration file.

Examples

Obtain the CA certificate from the certificate distribution server. (This operation requires the user to confirm the fingerprint of the root CA certificate.)

```
<Sysname> system-view
[Sysname] pki retrieve-certificate domain aaa ca
The trusted CA's finger print is:
    MD5  fingerprint:5C41 E657 A0D6 ECB4 6BD6 1823 7473 AABC
    SHA1 fingerprint:1616 E7A5 D89A 2A99 9419 1C12 D696 8228 87BC C266
Is the finger print correct?(Y/N):y
```

Obtain the local certificates from the certificate distribution server.

```
<Sysname> system-view
[Sysname] pki retrieve-certificate domain aaa local
```

Obtain the certificate of the peer entity **en1** from the certificate distribution server.

```
<Sysname> system-view
[Sysname] pki retrieve-certificate domain aaa peer en1
```

Related commands

`display pki certificate`

`pki delete-certificate`

pki retrieve-crl

Use **`pki retrieve-crl`** to obtain CRLs and save them locally.

Syntax

`pki retrieve-crl domain` *`domain-name`*

Views

System view

Predefined user roles

network-admin

Parameters

`domain-name`: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in Table 16.

Table 16 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

Usage guidelines

CRLs are used to verify the validity of the local certificates and the peer certificates in a PKI domain. To obtain CRLs, a PKI domain must have the correct CA certificate.

The URL of the CRL repository is specified by using the **crl url** command.

The device can obtain CRLs from the CRL repository through the HTTP, LDAP, or SCEP protocol. Which protocol is used depends on the configuration of the CRL repository in the PKI domain:

- If the specified URL of the CRL repository is in HTTP format, the device obtains CRLs through the HTTP protocol.
- If the specified URL of the CRL repository is in LDAP format, the device obtains CRLs through the LDAP protocol. If the specified URL does not have a host name, for example, ldap:///CN=8088,OU=test,U=rd,C=cn, you must specify the LDAP server's URL for the PKI domain by using the **ldap server** command. The device can obtain the complete URL of the LDAP repository by combining the URLs of the LDAP server and of the CRL repository.
- If the PKI domain is not configured with the CRL repository, the device looks up the local certificates and then the CA certificate for the CRL repository. If a CRL repository is found, the device obtains CRLs from the CRL repository. If no CRL repository is found, the device obtains CRLs through the SCEP protocol.

Examples

Obtain CRLs from the CRL repository.

```
<Sysname> system-view
[Sysname] pki retrieve-crl domain aaa
```

Related commands

crl url

ldap server

pki storage

Use **pki storage** to specify the storage path for the certificates or CRLs.

Use **undo pki storage** to restore the default.

Syntax

pki storage { **certificates** | **crls** } *dir-path*

undo pki storage { **certificates** | **crls** }

Default

Certificates and CRLs are stored in the **PKI** directory on the storage media of the device. The **PKI** directory is automatically created when a certificate is successfully requested, obtained, or imported for the first time.

Views

System view

Predefined user roles

network-admin

Parameters

certificates: Specifies a storage path for certificates.

crls: Specifies a storage path for CRLs.

dir-path: Specifies a storage path, a case-sensitive string, which cannot start with a slash (/) or contain two dots plus a slash (../). The *dir-path* argument specifies an absolute path or a relative path, and the path must exist.

Usage guidelines

The specified storage path must be on the master device.

If the path to be specified does not exist, use the **mkdir** command to create the path first.

Certificate files use the .cer or .p12 file extension. CRL files use the .crl file extension. After you change the storage path for certificates or CRLs, the certificate files and CRL files in the original path are moved to the new path.

Examples

Specifies **flash:/pki-new** as the storage path for certificates.

```
<Sysname> system-view
[Sysname] pki storage certificates flash:/pki-new
```

Specifies **pki-new** as the storage path for CRLs.

```
<Sysname> system-view
[Sysname] pki storage crls pki-new
```

pki validate-certificate

Use **pki validate-certificate** to verify the validity of certificates.

Syntax

pki validate-certificate domain *domain-name* { **ca** | **local** }

Views

System view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in Table 17.

Table 17 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

ca: Specifies the CA certificate.

local: Specifies the local certificates.

Usage guidelines

Generally, certificates are automatically verified when you request, obtain, or import them, or when an application uses PKI.

You can also use this command to manually verify a certificate in the following aspects:

- Whether the certificate is issued by a trusted CA.
- Whether the certificate has expired.

- Whether the certificate is revoked. This check is performed only if CRL checking is enabled.

When CRL checking is enabled:

- To verify the local certificates, if the PKI domain has no CRLs, the device looks up the locally saved CRLs. If a correct CRL is found, the device loads the CRL to the PKI domain. If no correct CRL is found locally, the device obtains a correct CRL from the CA server and saves it locally.
- To verify the CA certificate, CRL checking is performed for the CA certificate chain from the current CA to the root CA.

Examples

Verify the validity of the CA certificate in PKI domain **aaa**.

```
<Sysname> system-view
[Sysname] pki validate-certificate domain aaa ca
Verifying certificate......
        Serial Number:
            f6:3c:15:31:fe:bb:ec:94:dc:3d:b9:3a:d9:07:70:e5
        Issuer:
            C=cn
            O=ccc
            OU=ppp
            CN=rootca
        Subject:
            C=cn
            O=abc
            OU=test
            CN=aca

Verify result: OK
Verifying certificate......
        Serial Number:
            5c:72:dc:c4:a5:43:cd:f9:32:b9:c1:90:8f:dd:50:f6
        Issuer:
            C=cn
            O=ccc
            OU=ppp
            CN=rootca
        Subject:
            C=cn
            O=ccc
            OU=ppp
            CN=rootca

Verify result: OK
```

Verify the local certificates in PKI domain **aaa**.

```
<Sysname> system-view
[Sysname] pki validate-certificate domain aaa local
Verifying certificate......
        Serial Number:
            bc:05:70:1f:0e:da:0d:10:16:1e
        Issuer:
```

```
            C=CN
            O=sec
            OU=software
            CN=bca
        Subject:
            O=OpenCA Labs
            OU=Users
            CN=fips fips-sec

    Verify result: OK
```

Related commands

crl check

pki domain

public-key dsa

Use **public-key dsa** to specify a DSA key pair for certificate request.

Use **undo public-key** to restore the default.

Syntax

public-key dsa name *key-name* [**length** *key-length*]

undo public-key

Default

No key pair is specified for certificate request.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

name *key-name*: Specifies a key pair by its name, a case-insensitive string of 1 to 64 characters. The key pair name can contain only letters, digits, and hyphens (-).

length *key-length*: Specifies the key length, in bits. In non-FIPS mode, the value range is 512 to 2048, and the default is 1024. In FIPS mode, the value must be 2048. A longer key means higher security but more public key calculation time.

Usage guidelines

You can specify a nonexistent key pair in this command. A key pair can be obtained in any of the following ways:

- Use the **public-key local create** command to generate a key pair.
- An application, like IKE using digital signature authentication, triggers the device to generate a key pair.
- Use the **pki import** command to import a certificate containing a key pair.

A PKI domain can have key pairs using only one type of cryptographic algorithm (DSA, ECDSA, or RSA).

If you configure a DSA key pair for a PKI domain multiple times, the most recent configuration takes effect.

The **length** *key-length* option takes effect only if you specify a nonexistent key pair. The device will automatically create the key pair by using the specified name and length before submitting a certificate request. The **length** *key-length* option is ignored if the specified key pair already exists or is already contained in an imported certificate.

Examples

Specify 2048-bit DSA key pair **abc** for certificate request.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] public-key dsa name abc length 2048
```

Related commands

pki import

public-key local create

public-key ecdsa

Use **public-key ecdsa** to specify an ECDSA key pair for certificate request.

Use **undo public-key** to restore the default.

Syntax

In non-FIPS mode:

public-key ecdsa name *key-name* [**secp192r1** | **secp256r1** | **secp384r1** | **secp521r1**]

undo public-key

In FIPS mode:

public-key ecdsa name *key-name* [**secp256r1** | **secp384r1** | **secp521r1**]

undo public-key

Default

No key pair is specified for certificate request.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

name *key-name*: Specifies a key pair by its name, a case-insensitive string of 1 to 64 characters. The key pair name can contain only letters, digits, and hyphens (-).

secp192r1: Uses the secp192r1 curve to generate the key pair.

secp256r1: Uses the secp256r1 curve to generate the key pair.

secp384r1: Uses the secp384r1 curve to generate the key pair.

secp521r1: Uses the secp521r1 curve to generate the key pair.

Usage guidelines

You can specify a nonexistent key pair for a PKI domain.

A key pair can be obtained in any of the following ways:

- Use the **public-key local create** command to generate a key pair.
- An application, like IKE using digital signature authentication, triggers the device to generate a key pair.
- Use the **pki import** command to import a certificate containing a key pair.

A PKI domain can have key pairs using only one type of cryptographic algorithm (DSA, ECDSA, or RSA).

If you configure an ECDSA key pair for a PKI domain multiple times, the most recent configuration takes effect.

The specified elliptic curve takes effect only if you specify a nonexistent key pair. The device will automatically create the key pair by using the specified name and curve before submitting a certificate request. The curve parameter is ignored if the specified key pair already exists or is already contained in an imported certificate.

If you do not specify an elliptic curve, the secp192r1 curve is used by default in non-FIPS mode and the secp256r1 curve is used by default in FIPS mode.

Examples

Specify 384-bit ECDSA key pair **abc** for certificate request.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] public-key ecdsa name abc secp384r1
```

Related commands

pki import

public-key local create

public-key rsa

Use **public-key rsa** to specify an RSA key pair for certificate request.

Use **undo public-key** to restore the default.

Syntax

public-key rsa { { **encryption name** *encryption-key-name* [**length** *key-length*] | **signature name** *signature-key-name* [**length** *key-length*] } * | **general name** *key-name* [**length** *key-length*] }

undo public-key

Default

No key pair is specified for certificate request.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

encryption: Specifies a key pair for encryption.

name *encryption-key-name*: Specifies a key pair name, a case-insensitive string of 1 to 64 characters. The key pair name can contain only letters, digits, and hyphens (-).

signature: Specifies a key pair for signing.

name *signature-key-name*: Specifies a key pair name, a case-insensitive string of 1 to 64 characters. The key pair name can contain only letters, digits, and hyphens (-).

general: Specifies a key pair for both signing and encryption.

name *key-name*: Specifies a key pair name, a case-insensitive string of 1 to 64 characters. The key pair name can contain only letters, digits, and hyphens (-).

length *key-length*: Specifies the key length, in bits. In non-FIPS mode, the value range is 512 to 4096, and the default is 1024. In FIPS mode, the value must be a multiple of 256 in the range of 2048 to 4096, and the default is 2048. A longer key means higher security but more public key calculation time.

Usage guidelines

You can specify a nonexistent key pair in this command. You can get a key pair in any of the following ways:

- Use the **public-key local create** command to generate a key pair.
- An application, like IKE using digital signature authentication, triggers the device to generate a key pair.
- Use the **pki import** command to import a certificate containing a key pair.

A PKI domain can have key pairs using only one type of cryptographic algorithm (DSA, ECDSA, or RSA).

A PKI domain can have two RSA key pairs of different purposes: one is the signing key pair, and the other is the encryption key pair. If you configure an RSA signing key pair or RSA encryption key pair multiple times, the most recent configuration takes effect. The RSA signing key pair and encryption key pair do not overwrite each other.

If you specify a signing key pair and an encryption key pair separately, their key length can be different.

The **length** *key-length* option takes effect only if you specify a nonexistent key pair. The device will automatically create the key pair by using the specified name and length before submitting a certificate request. The **length** *key-length* option is ignored if the specified key pair already exists or is already contained in an imported certificate.

Examples

Specify 2048-bit general purpose RSA key pair **abc** for certificate request.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] public-key rsa general name abc length 2048
```

Specify the following RSA key pairs for certificate request:

- 2048-bit RSA encryption key pair **rsa1**.
- 2048-bit RSA signing key pair **sig1**.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] public-key rsa encryption name rsa1 length 2048
[Sysname-pki-domain-aaa] public-key rsa signature name sig1 length 2048
```

Related commands

pki import

public-key local create

root-certificate fingerprint

Use **root-certificate fingerprint** to set the fingerprint for verifying the root CA certificate.

Use **undo root-certificate fingerprint** to restore the default.

Syntax

In non-FIPS mode:

root-certificate fingerprint { **md5** | **sha1** } *string*

undo root-certificate fingerprint

In FIPS mode:

root-certificate fingerprint sha1 *string*

undo root-certificate fingerprint

Default

No fingerprint is set for verifying the root CA certificate.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

md5: Sets an MD5 fingerprint.

sha1: Sets an SHA1 fingerprint.

string: Sets the fingerprint in hexadecimal notation. If you specify the **MD5** keyword, the fingerprint is a string of 32 characters. If you specify the **SHA1** keyword, the fingerprint is a string of 40 characters.

Usage guidelines

If you set the certificate request mode to auto for a PKI domain that does not have a CA certificate, you must configure the fingerprint for root CA certificate verification. When an application (for example, IKE) triggers the device to request local certificates, the device automatically performs the following operations:

1. Obtains the CA certificate from the CA server.
2. Compares the fingerprint contained in the root CA certificate with the fingerprint configured in the PKI domain, if either of the following conditions exists:
   - The obtained CA certificate is a root certificate.
   - The obtained CA certificate is a certificate chain and contains a root certificate that does not exist on the device.

   If the two fingerprints do not match, or if no fingerprint is configured in the PKI domain, the device rejects the CA certificate and the local certificate request fails.

The fingerprint configured by this command is also used for root CA certificate verification when the device performs the following operations:

- Imports the CA certificate as requested by the **pki import** command.
- Obtains the CA certificate as requested by the **pki retrieve-certificate** command.

The device compares the fingerprint contained in the root CA certificate with the fingerprint configured in the PKI domain, if either of the following conditions exists:

- The CA certificate to be imported or obtained is a root certificate that does not exist on the device.
- The CA certificate to be imported or obtained is a certificate chain and contains a root certificate that does not exist on the device.

If the two fingerprints do not match, the device rejects the CA certificate. If no fingerprint is configured in the PKI domain, the device prompts you to manually verify the fingerprint of the root CA certificate.

Examples

Specify an MD5 fingerprint for verifying the root CA certificate. (This feature is supported only in non-FIPS mode.)

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] root-certificate fingerprint md5
12EF53FA355CD23E12EF53FA355CD23E
```

Specify an SHA1 fingerprint for verifying the root CA certificate.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] root-certificate fingerprint sha1
D1526110AAD7527FB093ED7FC037B0B3CDDDAD93
```

Related commands

certificate request mode

pki import

pki retrieve-certificate

rule

Use **rule** to create an access control rule.

Use **undo rule** to remove an access control rule.

Syntax

rule [*id*] { **deny** | **permit** } *group-name*

undo rule *id*

Default

No access control rules exist.

Views

Certificate-based access control policy view

Predefined user roles

network-admin

Parameters

id: Assigns an ID to the access control rule, in the range of 1 to 16. The default setting is the smallest unused ID in this range.

deny: Denies the certificates that match the associated attribute group.

permit: Permits the certificates that match the associated attribute group.

group-name: Specifies a certificate attribute group by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

When you create an access control rule, you can associate it with a nonexistent certificate attribute group.

The system determines that a certificate matches an access control rule when either of the following conditions exists:

- The associated certificate attribute group does not exist.
- The associated certificate attribute group does not contain any attribute rules.
- The certificate matches all attribute rules in the associated certificate attribute group.

You can configure multiple access control rules for an access control policy. A certificate matches the rules one by one, starting with the rule with the smallest ID. When a match is found, the match process stops, and the system performs the access control action defined in the access control rule.

Examples

Create rule 1 to permit all certificates that match certificate attribute group **mygroup**.

```
<Sysname> system-view
[Sysname] pki certificate access-control-policy mypolicy
[Sysname-pki-cert-acp-mypolicy] rule 1 permit mygroup
```

Related commands

attribute

display pki certificate access-control-policy

pki certificate attribute-group

source

Use **source** to specify the source IP address for PKI protocol packets.

Use **undo source** to restore the default.

Syntax

source { **ip** | **ipv6** } { *ip-address* | **interface** *interface-type interface-number* }

undo source

Default

The source IP address of PKI protocol packets is the IP address of their outgoing interface.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

ip *ip-address*: Specifies a source IPv4 address.

ipv6 *ip-address*: Specifies a source IPv6 address.

interface *interface-type interface-number*: Specifies an interface by its type and number. The interface's primary IP address or the lowest IPv6 address will be used as the source IP address for PKI protocol packets.

Usage guidelines

Use this command to specify the source IP address for PKI protocol packets. You can also specify a source interface if the IP address is dynamically obtained.

Make sure there is a route between the source IP address and the CA server.

You can specify only one source IP address in a PKI domain. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify **111.1.1.8** as the source IP address for PKI protocol packets.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] source ip 111.1.1.8
```

Specify **1::8** as the source IPv6 address for PKI protocol packets.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] source ipv6 1::8
```

Use the IP address of VLAN-interface 1 as the source IP address for PKI protocol packets.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] source ip interface vlan-interface 1
```

Use the IPv6 address of VLAN-interface 1 as the source IPv6 address for PKI protocol packets.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] source ipv6 interface vlan-interface 1
```

state

Use **state** to set the state or province name for a PKI entity.

Use **undo state** to restore the default.

Syntax

state *state-name*

undo state

Default

No state name or province name is set for a PKI entity.

Views

PKI entity view

Predefined user roles

network-admin

Parameters

state-name: Specifies a state or province by its name, a case-sensitive string of 1 to 63 characters. No comma can be included.

Examples

Set the state name to **countryA** for PKI entity **en**.

```
<Sysname> system-view
```

```
[Sysname] pki entity en
[Sysname-pki-entity-en] state countryA
```

usage

Use **usage** to specify the extensions for certificates.

Use **undo usage** to remove certificate extensions.

Syntax

usage { **ike** | **ssl-client** | **ssl-server** } *

undo usage [**ike** | **ssl-client** | **ssl-server**] *

Default

No extensions for certificates are specified. A certificate can be used for IKE, SSL clients, and SSL servers.

Views

PKI domain view

Predefined user roles

network-admin

Parameters

ike: Specifies the IKE certificate extension so IKE peers can use the certificates.

ssl-client: Specifies the SSL client certificate extension so the SSL client can use the certificates.

ssl-server: Specifies the SSL server certificate extension so the SSL server can use the certificates.

Usage guidelines

If you do not specify any keywords for the **undo usage** command, this command removes all certificate extensions.

The extension options contained in a certificate depends on the CA policy, and might be different from those specified in the PKI domain.

Examples

Specify the IKE certificate extension.

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] usage ike
```

Contents

IPsec commands

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

ah authentication-algorithm

Use **ah authentication-algorithm** to specify authentication algorithms for the AH protocol.

Use **undo ah authentication-algorithm** to restore the default.

Syntax

In non-FIPS mode:

ah authentication-algorithm { **aes-xcbc-mac** | **md5** | **sha1** | **sha256** | **sha384** | **sha512** } *

undo ah authentication-algorithm

In FIPS mode:

ah authentication-algorithm { **sha1**| **sha256** | **sha384** | **sha512** } *

undo ah authentication-algorithm

Default

AH does not use any authentication algorithms.

Views

IPsec transform set view

Predefined user roles

network-admin

Parameters

aes-xcbc-mac: Specifies the HMAC-AES-XCBC-96 algorithm, which uses a 128-bit key. This keyword is available only for IKEv2.

md5: Specifies the HMAC-MD5-96 algorithm, which uses a 128-bit key.

sha1: Specifies the HMAC-SHA1-96 algorithm, which uses a 160-bit key.

sha256: Specifies the HMAC-SHA256 algorithm, which uses a 256-bit key.

sha384: Specifies the HMAC-SHA384 algorithm, which uses a 384-bit key.

sha512: Specifies the HMAC-SHA512 algorithm, which uses a 512-bit key.

Usage guidelines

In non-FIPS mode, you can specify multiple AH authentication algorithms for one IPsec transform set, and the algorithm specified earlier has a higher priority.

For a manual or IKEv1-based IPsec policy, the first specified AH authentication algorithm takes effect. To make sure an IPsec tunnel can be established successfully, the IPsec transform sets specified at both ends of the tunnel must have the same first AH authentication algorithm.

Examples

Specify HMAC-SHA1 as the AH authentication algorithm for IPsec transform set **tran1**.

```
<Sysname> system-view
```

```
[Sysname] ipsec transform-set tran1
[Sysname-ipsec-transform-set-tran1] ah authentication-algorithm sha1
```

description

Use **description** to configure a description for an IPsec policy, IPsec policy template, or IPsec profile.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

No description is configured for an IPsec policy, IPsec policy template, or IPsec profile.

Views

IPsec policy view

IPsec policy template view

IPsec profile view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 80 characters.

Usage guidelines

If the system has multiple IPsec policies, IPsec policy templates, or IPsec profiles, you can use this command to configure different descriptions for them to distinguish them.

Examples

Configure the description for IPsec policy **policy1** as **CenterToA**.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 1 isakmp
[Sysname-ipsec-policy-isakmp-policy1-1] description CenterToA
```

display ipsec { ipv6-policy | policy }

Use **display ipsec** { **ipv6-policy** | **policy** } to display information about IPsec policies.

Syntax

display ipsec { **ipv6-policy** | **policy** } [*policy-name* [*seq-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6-policy: Displays information about IPv6 IPsec policies.

policy: Displays information about IPv4 IPsec policies.

policy-name: Specifies an IPsec policy by its name, a case-insensitive string of 1 to 63 characters.

seq-number: Specifies an IPsec policy entry by its sequence number in the range of 1 to 65535.

Usage guidelines

If you do not specify any parameters, this command displays information about all IPsec policies.

If you specify an IPsec policy name and a sequence number, this command displays information about the specified IPsec policy entry. If you specify an IPsec policy name without any sequence number, this command displays information about all IPsec policy entries with the specified name.

Examples

Display information about all IPv4 IPsec policies.

```
<Sysname> display ipsec policy
-----------------------------------------
IPsec Policy: mypolicy
-----------------------------------------

  ----------------------------
  Sequence number: 1
  Mode: Manual
  ----------------------------
  The policy configuration is incomplete:
           ACL not specified
           Incomplete transform-set configuration
  Description: This is my first IPv4 manual policy
  Security data flow:
  Remote address: 2.5.2.1
  Transform set: transform

  Inbound AH setting:
    AH SPI: 1200 (0x000004b0)
    AH string-key: ******
    AH authentication hex key:

  Inbound ESP setting:
    ESP SPI: 1400 (0x00000578)
    ESP string-key:
    ESP encryption hex key:
    ESP authentication hex key:

  Outbound AH setting:
    AH SPI: 1300 (0x00000514)
    AH string-key: ******
    AH authentication hex key:
```

```
  Outbound ESP setting:
    ESP SPI: 1500 (0x000005dc)
    ESP string-key: ******
    ESP encryption hex key:
    ESP authentication hex key:

  ----------------------------
  Sequence number: 2
  Mode: ISAKMP
  ----------------------------
  The policy configuration is incomplete:
           Remote-address not set
           ACL not specified
           Transform-set not set
  Description: This is my first IPv4 Isakmp policy
  Traffic Flow Confidentiality: Enabled
  Security data flow:
  Selector mode: standard
  Local address:
  Remote address:
  Transform set:
  IKE profile:
  IKEv2 profile:
  SA duration(time based): 3600 seconds
  SA duration(traffic based): 1843200 kilobytes
  SA idle time:
------------------------------------------
IPsec Policy: mycompletepolicy
Interface: LoopBack2
------------------------------------------

  ----------------------------
  Sequence number: 1
  Mode: Manual
  ----------------------------
  Description: This is my complete policy
  Security data flow: 3100
  Remote address: 2.2.2.2
  Transform set: completetransform

  Inbound AH setting:
    AH SPI: 5000 (0x00001388)
    AH string-key: ******
    AH authentication hex key:

  Inbound ESP setting:
    ESP SPI: 7000 (0x00001b58)
    ESP string-key: ******
```

```
    ESP encryption hex key:
    ESP authentication hex key:

  Outbound AH setting:
    AH SPI: 6000 (0x00001770)
    AH string-key: ******
    AH authentication hex key:

  Outbound ESP setting:
    ESP SPI: 8000 (0x00001f40)
    ESP string-key: ******
    ESP encryption hex key:
    ESP authentication hex key:

  ----------------------------
  Sequence number: 2
  Mode: ISAKMP
  ----------------------------
  Description: This is my complete policy
  Traffic Flow Confidentiality: Enabled
  Security data flow: 3200
  Selector mode: standard
  Local address:
  Remote address: 5.3.6.9
  Transform set:  completetransform
  IKE profile:
  IKEv2 profile:
  SA duration(time based): 3600 seconds
  SA duration(traffic based): 1843200 kilobytes
  SA idle time:
```

Display information about all IPv6 IPsec policies.

```
<Sysname> display ipsec ipv6-policy
-----------------------------------------
IPsec Policy: mypolicy
-----------------------------------------

  ----------------------------
  Sequence number: 1
  Mode: Manual
  ----------------------------
  Description: This is my first IPv6 policy
  Security data flow: 3600
  Remote address: 1000::2
  Transform set: mytransform

  Inbound AH setting:
    AH SPI: 1235 (0x000004d3)
    AH string-key: ******
```

```
    AH authentication hex key:

  Inbound ESP setting:
    ESP SPI: 1236 (0x000004d4)
    ESP string-key: ******
    ESP encryption hex key:
    ESP authentication hex key:

  Outbound AH setting:
    AH SPI: 1237 (0x000004d5)
    AH string-key: ******
    AH authentication hex key:

  Outbound ESP setting:
    ESP SPI: 1238 (0x000004d6)
    ESP string-key: ******
    ESP encryption hex key:
    ESP authentication hex key:
```

Table 1 Command output

Field	Description
IPsec Policy	IPsec policy name.
Interface	Interface applied with the IPsec policy.
Sequence number	Sequence number of the IPsec policy entry.
Mode	Negotiation mode of the IPsec policy: • **Manual**—Manual mode. • **ISAKMP**—IKE negotiation mode. • **Template**—IPsec policy template mode.
The policy configuration is incomplete	IPsec policy configuration incomplete. Possible causes include: • The ACL is not configured. • The IPsec transform set is not configured. • The ACL does not have any **permit** statements. • The IPsec transform set configuration is not complete. • The peer IP address of the IPsec tunnel is not specified. • The SPI and key of the IPsec SA do not match those in the IPsec policy.
Description	Description of the IPsec policy.
Traffic Flow Confidentiality	Whether Traffic Flow Confidentiality (TFC) padding is enabled.
Security data flow	ACL used by the IPsec policy.
Selector mode	Data flow protection mode of the IPsec policy: **standard**, **aggregation**, or **per-host**.
Local address	Local end IP address of the IPsec tunnel (available only for the IKE-based IPsec policy).
Remote address	Remote end IP address or host name of the IPsec tunnel.
Transform set	Transform set used by the IPsec policy.
IKE profile	IKE profile used by the IPsec policy.

Field	Description
IKEv2 profile	IKEv2 profile used by the IPsec policy.
SA duration(time based)	Time-based IPsec SA lifetime, in seconds.
SA duration(traffic based)	Traffic-based IPsec SA lifetime, in kilobytes.
SA idle time	Idle timeout of the IPsec SA, in seconds.
AH string-key	AH string key. This field displays ****** if the key is configured and it is empty if the key is not configured.
AH authentication hex key	AH authentication hexadecimal key. This field displays ****** if the key is configured and it is empty if the key is not configured.
ESP string-key	ESP string key. This field displays ****** if the key is configured and it is empty if the key is not configured.
ESP encryption hex key	ESP encryption hexadecimal key. This field displays ****** if the key is configured and it is empty if the key is not configured.
ESP authentication hex key	ESP authentication hexadecimal key. This field displays ****** if the key is configured and it is empty if the key is not configured.

Related commands

ipsec { ipv6-policy | policy }

display ipsec { ipv6-policy-template | policy-template }

Use **display ipsec** { **ipv6-policy-template** | **policy-template** } to display information about IPsec policy templates

Syntax

display ipsec { **ipv6-policy-template** | **policy-template** } [*template-name* [*seq-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6-policy-template: Displays information about IPv6 IPsec policy templates.

policy-template: Displays information about IPv4 IPsec policy templates.

template-name: Specifies an IPsec policy template by its name, a case-insensitive string of 1 to 63 characters.

seq-number: Specifies an IPsec policy template entry by its sequence number in the range of 1 to 65535.

Usage guidelines

If you do not specify any parameters, this command displays information about all IPsec policy templates.

If you specify an IPsec policy template name and a sequence number, this command displays information about the specified IPsec policy template entry. If you specify an IPsec policy template

name without any sequence number, this command displays information about all IPsec policy template entries with the specified name.

Examples

Display information about all IPv4 IPsec policy templates.

```
<Sysname> display ipsec policy-template
-----------------------------------------------
IPsec Policy Template: template
-----------------------------------------------

  --------------------------------
  Sequence number: 1
  --------------------------------
Description: This is policy template
Traffic Flow Confidentiality: Disabled
Security data flow :
Selector mode: standard
Local address:
IKE profile:
IKEv2 profile:
Remote address: 162.105.10.2
Transform set:  testprop
IPsec SA local duration(time based): 3600 seconds
IPsec SA local duration(traffic based): 1843200 kilobytes
SA idle time:
```

Display information about all IPv6 IPsec policy templates.

```
<Sysname> display ipsec ipv6-policy-template
-----------------------------------------------
IPsec Policy Template: template6
-----------------------------------------------

  --------------------------------
  Sequence number: 1
  --------------------------------
Description: This is policy template
Traffic Flow Confidentiality: Disabled
Security data flow :
Selector mode: standard
Local address:
IKE profile:
IKEv2 profile:
Remote address: 200::1
Transform set: testprop
IPsec SA local duration(time based): 3600 seconds
IPsec SA local duration(traffic based): 1843200 kilobytes
SA idle time:
```

Table 2 Command output

Field	Description
IPsec Policy Template	IPsec policy template name.
Sequence number	Sequence number of the IPsec policy template entry.
Description	Description of the IPsec policy template.
Traffic Flow Confidentiality	Whether Traffic Flow Confidentiality (TFC) padding is enabled.
Security data flow	ACL used by the IPsec policy template.
Selector mode	Data flow protection mode of the IPsec policy template: **standard**, **aggregation**, or **per-host**.
Local address	Local end IP address of the IPsec tunnel.
IKE profile	IKE profile used by the IPsec policy template.
IKEv2 profile	IKEv2 profile used by the IPsec policy template.
Remote address	Remote end IP address of the IPsec tunnel.
Transform set	Transform set used by the IPsec policy template.
IPsec SA local duration(time based)	Time-based IPsec SA lifetime, in seconds.
IPsec SA local duration(traffic based)	Traffic-based IPsec SA lifetime, in kilobytes.
SA idle time	Idle timeout of the IPsec SA, in seconds.

Related commands

ipsec { **ipv6-policy** | **policy** } **isakmp template**

display ipsec profile

Use **display ipsec profile** to display information about IPsec profiles.

Syntax

display ipsec profile [*profile-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

profile-name: Specifies an IPsec profile by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

If you do not specify any parameters, this command displays information about all IPsec profiles.

Examples

Display information about all IPsec profiles.

```
<Sysname> display ipsec profile
-----------------------------------------------
```

```
IPsec profile: profile
Mode: manual
-----------------------------------------------
  Transform set: prop1

  Inbound AH setting:
    AH SPI: 12345 (0x00003039)
    AH string-key:
    AH authentication hex key: ******
  Inbound ESP setting:
    ESP SPI: 23456 (0x00005ba0)
    ESP string-key:
    ESP encryption hex-key: ******
    ESP authentication hex-key: ******
  Outbound AH setting:
    AH SPI: 12345 (0x00003039)
    AH string-key:
    AH authentication hex key: ******
  Outbound ESP setting:
    ESP SPI: 23456 (0x00005ba0)
    ESP string-key:
    ESP encryption hex key: ******
    ESP authentication hex key: ******
```

Table 3 Command output

Field	Description
IPsec profile	IPsec profile name.
Mode	Negotiation mode used by the IPsec profile.
Description	Description of the IPsec profile.
Transform set	IPsec transform set used by the IPsec profile.

Related commands

ipsec profile

display ipsec sa

Use **display ipsec sa** to display information about IPsec SAs.

Syntax

display ipsec sa [**brief** | **count** | **interface** *interface-type interface-number* | { **ipv6-policy** | **policy** } *policy-name* [*seq-number*] | **profile** *profile-name* | **remote** [**ipv6**] *ip-address*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

brief: Displays brief information about all IPsec SAs.

count: Displays the number of IPsec SAs.

interface *interface-type interface-number*: Specifies an interface by its type and number.

ipv6-policy: Displays detailed information about IPsec SAs created by using a specified IPv6 IPsec policy.

policy: Displays detailed information about IPsec SAs created by using a specified IPv4 IPsec policy.

policy-name: Specifies an IPsec policy by its name, a case-insensitive string of 1 to 63 characters.

seq-number: Specifies an IPsec policy entry by its sequence number. The value range is 1 to 65535.

profile: Displays detailed information about IPsec SAs created by using a specified IPsec profile.

profile-name: Specifies an IPsec profile by its name, a case-insensitive string of 1 to 63 characters.

remote *ip-address*: Specifies an IPsec SA by its remote end IP address.

ipv6: Specifies an IPsec SA by its remote end IPv6 address. If this keyword is not specified, the specified remote end IP address is an IPv4 address.

Usage guidelines

If you do not specify any parameters, this command displays detailed information about all IPsec SAs.

Examples

Display brief information about IPsec SAs.

```
<Sysname> display ipsec sa brief
-------------------------------------------------------------------------
Interface/Global   Dst Address      SPI         Protocol  Status
-------------------------------------------------------------------------
Vlan100            10.1.1.1         400         ESP       Active
Vlan100            255.255.255.255  4294967295  ESP       Active
Vlan100            100::1/64        500         AH        Active
Global             --               600         ESP       Active
```

Table 4 Command output

Field	Description
Interface/Global	Interface where the IPsec SA belongs to or global IPsec SA (created by using an IPsec profile).
Dst Address	Remote end IP address of the IPsec tunnel. For the IPsec SAs created by using IPsec profiles, this field displays two hyphens (**--**).
SPI	IPsec SA SPI.
Protocol	Security protocol used by IPsec.
Status	Status of the IPsec SA, which can only be **Active**.

Display the number of IPsec SAs.

```
<Sysname> display ipsec sa count
Total IPsec SAs count: 4
```

Display detailed information about all IPsec SAs.

```
<Sysname> display ipsec sa
-------------------------------
Interface: Vlan-interface100
-------------------------------

  ----------------------------
  IPsec policy: r2
  Sequence number: 1
  Mode: ISAKMP
  ----------------------------
    Tunnel id: 3
    Encapsulation mode: tunnel
    Perfect Forward Secrecy:
    Inside VRF: vp1
    Extended Sequence Numbers enable: Y
    Traffic Flow Confidentiality enable: N
    Path MTU: 1443
    Tunnel:
        local  address: 2.2.2.2
        remote address: 1.1.1.2
    Flow:
        sour addr: 192.168.2.0/255.255.255.0  port: 0  protocol: ip
        dest addr: 192.168.1.0/255.255.255.0  port: 0  protocol: ip

    [Inbound ESP SAs]
      SPI: 3564837569 (0xd47b1ac1)
      Connection ID: 90194313219
      Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
      SA duration (kilobytes/sec): 4294967295/604800
      SA remaining duration (kilobytes/sec): 1843200/2686
      Max received sequence-number: 5
      Anti-replay check enable: Y
      Anti-replay window size: 32
      UDP encapsulation used for NAT traversal: N
      Status: Active

    [Outbound ESP SAs]
      SPI: 801701189 (0x2fc8fd45)
      Connection ID: 64424509441
      Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
      SA duration (kilobytes/sec): 4294967295/604800
      SA remaining duration (kilobytes/sec): 1843200/2686
      Max sent sequence-number: 6
      UDP encapsulation used for NAT traversal: N
      Status: Active
```

```
------------------------------
Global IPsec SA
------------------------------

  ----------------------------
  IPsec profile: profile
  Mode: Manual
  ----------------------------
    Encapsulation mode: transport
    [Inbound AH SA]
      SPI: 1234563 (0x0012d683)
      Connection ID: 64426789452
      Transform set: AH-SHA1
      No duration limit for this SA
    [Outbound AH SA]
      SPI: 1234563 (0x002d683)
      Connection ID: 64428999468
      Transform set: AH-SHA1
      No duration limit for this SA
```

Table 5 Command output

Field	Description
Interface	Interface where the IPsec SA belongs.
IPsec policy	Name of the IPsec policy.
IPsec profile	Name of the IPsec profile.
Sequence number	Sequence number of the IPsec policy entry.
Mode	Negotiation mode used by the IPsec policy: • **Manual**—Manual mode. • **ISAKMP**—IKE negotiation mode. • **Template**—IPsec policy template mode.
Tunnel id	IPsec tunnel ID.
Encapsulation mode	Encapsulation mode, transport or tunnel.
Perfect Forward Secrecy	Perfect Forward Secrecy (PFS) used by the IPsec policy for negotiation: • 768-bit Diffie-Hellman group (**dh-group1**). • 1024-bit Diffie-Hellman group (**dh-group2**). • 1536-bit Diffie-Hellman group (**dh-group5**). • 2048-bit Diffie-Hellman group (**dh-group14**). • 2048-bit and 256_bit subgroup Diffie-Hellman group (**dh-group24**). • 256-bit ECP Diffie-Hellman group (**dh-group19**). • 384-bit ECP Diffie-Hellman group (**dh-group20**).
Extended Sequence Numbers enable	Whether Extended Sequence Number (ESN) is enabled.
Traffic Flow Confidentiality enable	Whether Traffic Flow Confidentiality (TFC) padding is enabled.
Inside VRF	This field is not supported in the current software version.

Field	Description
	VPN instance to which the protected data flow belongs.
Path MTU	Path MTU of the IPsec SA.
Tunnel	Local and remote addresses of the IPsec tunnel.
local address	Local end IP address of the IPsec tunnel.
remote address	Remote end IP address of the IPsec tunnel.
Flow	Information about the data flow protected by the IPsec tunnel.
sour addr	Source IP address of the data flow.
dest addr	Destination IP address of the data flow.
port	Port number.
protocol	Protocol type: **ip** or **ipv6**.
SPI	SPI of the IPsec SA.
Connection ID	Identifier of the IPsec SA.
Transform set	Security protocol and algorithms used by the IPsec transform set.
SA duration (kilobytes/sec)	IPsec SA lifetime, in kilobytes or seconds.
SA remaining duration (kilobytes/sec)	Remaining IPsec SA lifetime, in kilobytes or seconds.
Max received sequence-number	Max sequence number in the received packets.
Max sent sequence-number	Max sequence number in the sent packets.
Anti-replay check enable	Whether anti-replay checking is enabled.
Status	Status of the IPsec SA, which can only be **Active**.
No duration limit for this SA	The manual IPsec SAs do not have lifetime.

Related commands

`ipsec sa global-duration`

`reset ipsec sa`

display ipsec statistics

Use **`display ipsec statistics`** to display IPsec packet statistics.

Syntax

`display ipsec statistics` [**`tunnel-id`** *`tunnel-id`*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

tunnel-id *tunnel-id*: Specifies an IPsec tunnel by its ID. The value range for the *tunnel-id* argument is 0 to 4294967295. You can use the **display ipsec tunnel brief** command to view the IDs of established IPsec tunnels.

Usage guidelines

If you do not specify any parameters, this command displays statistics for all IPsec packets.

Examples

Display statistics for all IPsec packets.

```
<Sysname> display ipsec statistics
  IPsec packet statistics:
    Received/sent packets: 47/64
    Received/sent bytes: 3948/5208
    Dropped packets (received/sent): 0/45

    Dropped packets statistics
      No available SA: 0
      Wrong SA: 0
      Invalid length: 0
      Authentication failure: 0
      Encapsulation failure: 0
      Decapsulation failure: 0
      Replayed packets: 0
      ACL check failure: 45
      MTU check failure: 0
      Loopback limit exceeded: 0
      Crypto speed limit exceeded: 0
```

Display statistics for the packets of IPsec tunnel 1.

```
<Sysname> display ipsec statistics tunnel-id 1
  IPsec packet statistics:
    Received/sent packets: 5124/8231
    Received/sent bytes: 52348/64356
    Dropped packets (received/sent): 0/0

    Dropped packets statistics
      No available SA: 0
      Wrong SA: 0
      Invalid length: 0
      Authentication failure: 0
      Encapsulation failure: 0
      Decapsulation failure: 0
      Replayed packets: 0
      ACL check failure: 0
      MTU check failure: 0
```

```
Loopback limit exceeded: 0
Crypto speed limit exceeded: 0
```

Table 6 Command output

Field	Description
Received/sent packets	Number of received/sent IPsec-protected packets.
Received/sent bytes	Number of bytes of received/sent IPsec-protected packets.
Dropped packets (received/sent)	Number of dropped IPsec-protected packets (received/sent).
No available SA	Number of packets dropped due to lack of available IPsec SA.
Wrong SA	Number of packets dropped due to wrong IPsec SA.
Invalid length	Number of packets dropped due to invalid packet length.
Authentication failure	Number of packets dropped due to authentication failure.
Encapsulation failure	Number of packets dropped due to encapsulation failure.
Decapsulation failure	Number of packets dropped due to decapsulation failure.
Replayed packets	Number of dropped replayed packets.
ACL check failure	Number of packets dropped due to ACL check failure.
MTU check failure	Number of packets dropped due to MTU check failure.
Loopback limit exceeded	Number of packets dropped due to loopback limit exceeded.
Crypto speed limit exceeded	Number of packets dropped due to crypto speed limit exceeded.

Related commands

`reset ipsec statistics`

display ipsec transform-set

Use **`display ipsec transform-set`** to display information about IPsec transform sets.

Syntax

`display ipsec transform-set` [*`transform-set-name`*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

`transform-set-name`: Specifies an IPsec transform set by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

If you do not specify an IPsec transform set, this command displays information about all IPsec transform sets.

Examples

Display information about all IPsec transform sets.

```
<Sysname> display ipsec transform-set
IPsec transform set: mytransform
  State: incomplete
  Encapsulation mode: tunnel
  ESN: Enabled
  PFS:
  Transform: ESP

IPsec transform set: completeTransform
  State: complete
  Encapsulation mode: transport
  ESN: Enabled
  PFS:
  Transform: AH-ESP
  AH protocol:
    Integrity: SHA1
  ESP protocol:
    Integrity: SHA1
    Encryption: AES-CBC-128
```

Table 7 Command output

Field	Description
IPsec transform set	Name of the IPsec transform set.
State	Whether the IPsec transform set is complete.
Encapsulation mode	Encapsulation mode used by the IPsec transform set: **transport** or **tunnel**.
ESN	Whether Extended Sequence Number (ESN) is enabled.
PFS	Perfect Forward Secrecy (PFS) used by the IPsec policy for negotiation: • 768-bit Diffie-Hellman group (**dh-group1**). • 1024-bit Diffie-Hellman group (**dh-group2**). • 1536-bit Diffie-Hellman group (**dh-group5**). • 2048-bit Diffie-Hellman group (**dh-group14**). • 2048-bit and 256_bit subgroup Diffie-Hellman group (**dh-group24**). • 256-bit ECP Diffie-Hellman group (**dh-group19**). • 384-bit ECP Diffie-Hellman group (**dh-group20**).
Transform	Security protocols used by the IPsec transform set: AH, ESP, or both. If both protocols are configured, IPsec uses ESP before AH.
AH protocol	AH settings.
ESP protocol	ESP settings.
Integrity	Authentication algorithm used by the security protocol.
Encryption	Encryption algorithm used by the security protocol.

Related commands

ipsec transform-set

display ipsec tunnel

Use **display ipsec tunnel** to display information about IPsec tunnels.

Syntax

display ipsec tunnel { **brief** | **count** | **tunnel-id** *tunnel-id* }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

brief: Displays brief information about IPsec tunnels.

count: Displays the number of IPsec tunnels.

tunnel-id *tunnel-id*: Specifies an IPsec tunnel by its ID. The value range for the *tunnel-id* argument is 0 to 4294967295.

Usage guidelines

IPsec is a Layer 3 VPN technology that transmits data in a secure channel established between two endpoints (such as two security gateways). Such a secure channel is usually called an IPsec tunnel.

Examples

Display brief information about all IPsec tunnels.

```
<Sysname> display ipsec tunnel brief
-------------------------------------------------------------------------------
Tunn-id   Src Address     Dst Address     Inbound SPI   Outbound SPI  Status
-------------------------------------------------------------------------------
0         --              --              1000          2000          Active
                                          3000          4000
1         1.2.3.1         2.2.2.2         5000          6000          Active
                                          7000          8000
```

Table 8 Command output

Field	Description
Src Address	Source IP address of the IPsec tunnel. For IPsec SAs created by using IPsec profiles, this field displays two hyphens (**--**).
Dst Address	Destination IP address of the IPsec tunnel. For IPsec SAs created by using IPsec profiles, this field displays two hyphens (**--**).
Inbound SPI	Valid SPI in the inbound direction of the IPsec tunnel. If the tunnel uses two security protocols, two SPIs in the inbound direction are displayed in two lines.
Outbound SPI	Valid SPI in the outbound direction of the IPsec tunnel. If the tunnel uses two security protocols, two SPIs in the outbound direction are displayed in two lines.
Status	Status of the IPsec SA, which can only be **Active**.

Display the number of IPsec tunnels.

```
<Sysname> display ipsec tunnel count
Total IPsec Tunnel Count: 2
```

Display detailed information about all IPsec tunnels.

```
<Sysname> display ipsec tunnel
Tunnel ID: 0
Status: Active
Perfect forward secrecy:
Inside vpn-instance:
SA's SPI:
    outbound:  2000        (0x000007d0)   [AH]
    inbound:   1000        (0x000003e8)   [AH]
    outbound:  4000        (0x00000fa0)   [ESP]
    inbound:   3000        (0x00000bb8)   [ESP]
Tunnel:
    local  address:
    remote address:
Flow:

Tunnel ID: 1
Status: Active
Perfect forward secrecy:
Inside vpn-instance:
SA's SPI:
    outbound:  6000        (0x00001770)   [AH]
    inbound:   5000        (0x00001388)   [AH]
    outbound:  8000        (0x00001f40)   [ESP]
    inbound:   7000        (0x00001b58)   [ESP]
Tunnel:
    local  address: 1.2.3.1
    remote address: 2.2.2.2
Flow:
    as defined in ACL3100
```

Display detailed information about IPsec tunnel 1.

```
<Sysname> display ipsec tunnel tunnel-id 1
Tunnel ID: 1
Status: Active
Perfect forward secrecy:
Inside vpn-instance:
SA's SPI:
    outbound:  6000        (0x00001770)   [AH]
    inbound:   5000        (0x00001388)   [AH]
    outbound:  8000        (0x00001f40)   [ESP]
    inbound:   7000        (0x00001b58)   [ESP]
Tunnel:
    local  address: 1.2.3.1
    remote address: 2.2.2.2
```

```
Flow:
    as defined in ACL 3100
```

Table 9 Command output

Field	Description
Tunnel ID	IPsec ID, used to uniquely identify an IPsec tunnel.
Status	IPsec tunnel status, which can only be **Active**.
Perfect forward secrecy	Perfect Forward Secrecy (PFS) used by the IPsec policy for negotiation: • 768-bit Diffie-Hellman group (**dh-group1**). • 1024-bit Diffie-Hellman group (**dh-group2**). • 1536-bit Diffie-Hellman group (**dh-group5**). • 2048-bit Diffie-Hellman group (**dh-group14**). • 2048-bit and 256_bit subgroup Diffie-Hellman group (**dh-group24**). • 256-bit ECP Diffie-Hellman group (**dh-group19**). • 384-bit ECP Diffie-Hellman group (**dh-group20**).
Inside vpn-instance	This field is not supported in the current software version. VPN instance to which the IPsec-protected data belongs.
SA's SPI	SPIs of the inbound and outbound SAs.
Tunnel	Local and remote addresses of the IPsec tunnel.
local address	Local end IP address of the IPsec tunnel.
remote address	Remote end IP address of the IPsec tunnel.
Flow	Information about the data flow protected by the IPsec tunnel, including source IP address, destination IP address, source port, destination port, and protocol.
as defined in ACL 3001	Range of data flow protected by the IPsec tunnel that is established manually. This information shows that the IPsec tunnel protects all data flows defined by ACL 3001.

encapsulation-mode

Use **encapsulation-mode** to set the encapsulation mode that the security protocol uses to encapsulate IP packets.

Use **undo encapsulation-mode** to restore the default.

Syntax

encapsulation-mode { **transport** | **tunnel** }

undo encapsulation-mode

Default

IP packets are encapsulated in tunnel mode.

Views

IPsec transform set view

Predefined user roles

network-admin

Parameters

transport: Uses the transport mode for IP packet encapsulation.

tunnel: Uses the tunnel mode for IP packet encapsulation.

Usage guidelines

IPsec supports the following encapsulation modes:

- **Transport mode**—The security protocols protect the upper layer data of an IP packet. Only the transport layer data is used to calculate the security protocol headers. The calculated security protocol headers and the encrypted data (only for ESP encapsulation) are placed after the original IP header. You can use the transport mode when end-to-end security protection is required (the secured transmission start and end points are the actual start and end points of the data). The transport mode is typically used for protecting host-to-host communications.
- **Tunnel mode**—The security protocols protect the entire IP packet. The entire IP packet is used to calculate the security protocol headers. The calculated security protocol headers and the encrypted data (only for ESP encapsulation) are encapsulated in a new IP packet. In this mode, the encapsulated packet has two IP headers. The inner IP header is the original IP header. The outer IP header is added by the network device that provides the IPsec service. You must use the tunnel mode when the secured transmission start and end points are not the actual start and end points of the data packets (for example, when two gateways provide IPsec but the data start and end points are two hosts behind the gateways). The tunnel mode is typically used for protecting gateway-to-gateway communications.

The IPsec transform sets at both ends of the IPsec tunnel must have the same encapsulation mode.

Examples

Configure IPsec transform set **tran1** to use the transport mode for IP packet encapsulation.

```
<Sysname> system-view
[Sysname] ipsec transform-set tran1
[Sysname-ipsec-transform-set-tran1] encapsulation-mode transport
```

Related commands

ipsec transform-set

esn enable

Use **esn enable** to enable the Extended Sequence Number (ESN) feature.

Use **undo esn enable** to disable the ESN feature.

Syntax

esn enable [**both**]

undo esn enable

Default

The ESN feature is disabled.

Views

IPsec transform set view

Predefined user roles

network-admin

Parameters

both: Specifies IPsec to support both extended sequence number and traditional sequence number. If you do not specify this keyword, IPsec only supports extended sequence number.

Usage guidelines

The ESN feature extends the sequence number length from 32 bits to 64 bits. This feature prevents the sequence number space from being exhausted when large volumes of data are transmitted at high speeds over an IPsec SA. If the sequence number space is not exhausted, the IPsec SA does not need to be renegotiated.

This feature must be enabled at both the initiator and the responder.

Examples

Enable the ESN feature in IPsec transform set **tran1**.

```
<Sysname> system-view
[Sysname] ipsec transform-set tran1
[Sysname-ipsec-transform-set-tran1] esn enable
```

Related commands

display ipsec transform-set

esp authentication-algorithm

Use **esp authentication-algorithm** to specify authentication algorithms for ESP.

Use **undo esp authentication-algorithm** to restore the default.

Syntax

In non-FIPS mode:

esp authentication-algorithm { **aes-xcbc-mac** | **md5** | **sha1** | **sha256** | **sha384** | **sha512** } *

undo esp authentication-algorithm

In FIPS mode:

esp authentication-algorithm { **sha1**| **sha256** | **sha384** | **sha512** } *

undo esp authentication-algorithm

Default

ESP does not use any authentication algorithms.

Views

IPsec transform set view

Predefined user roles

network-admin

Parameters

aes-xcbc-mac: Specifies the HMAC-AES-XCBC-96 algorithm, which uses a 128-bit key. This keyword is available only for IKEv2.

md5: Specifies the HMAC-MD5-96 algorithm, which uses a 128-bit key.

sha1: Specifies the HMAC-SHA1-96 algorithm, which uses a 160-bit key.

sha256: Specifies the HMAC-SHA256 algorithm, which uses a 256-bit key.

sha384: Specifies the HMAC-SHA384 algorithm, which uses a 384-bit key.

sha512: Specifies the HMAC-SHA512 algorithm, which uses a 512-bit key.

Usage guidelines

In non-FIPS mode, you can specify multiple ESP authentication algorithms for one IPsec transform set, and the algorithm specified earlier has a higher priority.

For a manual or IKEv1-based IPsec policy, the first specified ESP authentication algorithm takes effect. To make sure an IPsec tunnel can be established successfully, the IPsec transform sets specified at both ends of the tunnel must have the same first ESP authentication algorithm.

Examples

Configure IPsec transform set **tran1** to use the HMAC-SHA1 algorithm as the ESP authentication algorithm.

```
<Sysname> system-view
[Sysname] ipsec transform-set tran1
[Sysname-ipsec-transform-set-tran1] esp authentication-algorithm sha1
```

Related commands

ipsec transform-set

esp encryption-algorithm

Use **esp encryption-algorithm** to specify encryption algorithms for ESP.

Use **undo esp encryption-algorithm** to restore the default.

Syntax

In non-FIPS mode:

esp encryption-algorithm { **3des-cbc** | **aes-cbc-128** | **aes-cbc-192** | **aes-cbc-256** | **aes-ctr-128** | **aes-ctr-192** | **aes-ctr-256** | **camellia-cbc-128** | **camellia-cbc-192** | **camellia-cbc-256** | **des-cbc** | **gmac-128** | **gmac-192** | **gmac-256** | **gcm-128** | **gcm-192** | **gcm-256** | **null** } *

undo esp encryption-algorithm

In FIPS mode:

esp encryption-algorithm { **aes-cbc-128** | **aes-cbc-192** | **aes-cbc-256** | **aes-ctr-128** | **aes-ctr-192** | **aes-ctr-256** | **gmac-128** | **gmac-192** | **gmac-256** | **gcm-128** | **gcm-192** | **gcm-256** }*

undo esp encryption-algorithm

Default

ESP does not use any encryption algorithms.

Views

IPsec transform set view

Predefined user roles

network-admin

Parameters

3des-cbc: Specifies the 3DES algorithm in CBC mode, which uses a 168-bit key.

aes-cbc-128: Specifies the AES algorithm in CBC mode, which uses a 128-bit key.

aes-cbc-192: Specifies the AES algorithm in CBC mode, which uses a 192-bit key.

aes-cbc-256: Specifies the AES algorithm in CBC mode, which uses a 256-bit key.

aes-ctr-128: Specifies the AES algorithm in CTR mode, which uses a 128-bit key. This keyword is available only for IKEv2.

aes-ctr-192: Specifies the AES algorithm in CTR mode, which uses a 192-bit key. This keyword is available only for IKEv2.

aes-ctr-256: Specifies the AES algorithm in CTR mode, which uses a 256-bit key. This keyword is available only for IKEv2.

camellia-cbc-128: Specifies the Camellia algorithm in CBC mode, which uses a 128-bit key. This keyword is available only for IKEv2.

camellia-cbc-192: Specifies the Camellia algorithm in CBC mode, which uses a 192-bit key. This keyword is available only for IKEv2.

camellia-cbc-256: Specifies the Camellia algorithm in CBC mode, which uses a 256-bit key. This keyword is available only for IKEv2.

des-cbc: Specifies the DES algorithm in CBC mode, which uses a 64-bit key.

gmac-128: Specifies the GMAC algorithm, which uses a 128-bit key. This keyword is available only for IKEv2.

gmac-192: Specifies the GMAC algorithm, which uses a 192-bit key. This keyword is available only for IKEv2.

gmac-256: Specifies the GMAC algorithm, which uses a 256-bit key. This keyword is available only for IKEv2.

gcm-128: Specifies the GCM algorithm, which uses a 128-bit key. This keyword is available only for IKEv2.

gcm-192: Specifies the GCM algorithm, which uses a 192-bit key. This keyword is available only for IKEv2.

gcm-256: Specifies the GCM algorithm, which uses a 256-bit key. This keyword is available only for IKEv2.

null: Specifies the NULL algorithm, which means encryption is not performed.

Usage guidelines

You can specify multiple ESP encryption algorithms for one IPsec transform set, and the algorithm specified earlier has a higher priority.

For a manual or IKEv1-based IPsec policy, the first specified ESP encryption algorithm takes effect. To make sure an IPsec tunnel can be established successfully, the IPsec transform sets specified at both ends of the tunnel must have the same first ESP encryption algorithm.

GCM and GMAC algorithms are combined mode algorithms. GCM algorithms provide encryption and authentication services. GMAC algorithms only provide authentication service. Combined mode algorithms can be used only when ESP is used alone without AH. Combined mode algorithms cannot be used together with ordinary ESP authentication algorithms.

Examples

Configure IPsec transform set **tran1** to use the AES-CBC-128 algorithm as the ESP encryption algorithm.

```
<Sysname> system-view
[Sysname] ipsec transform-set tran1
[Sysname-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
```

Related commands

ipsec transform-set

ike-profile

Use **ike-profile** to specify an IKE profile for an IPsec policy, IPsec policy template, or IPsec profile.

Use **undo ike-profile** to restore the default.

Syntax

ike-profile *profile-name*

undo ike-profile

Default

No IKE profile is specified for an IPsec policy, IPsec policy template, or IPsec profile.

Views

IPsec policy view

IPsec policy template view

IPsec profile view

Predefined user roles

network-admin

Parameters

profile-name: Specifies an IKE profile by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

If no IKE profile is specified for an IPsec policy, IPsec policy template, or IPsec profile, the device selects an IKE profile configured in system view for negotiation. If no IKE profile is configured in system view, the device uses the global IKE settings.

The IKE profile specified for an IPsec policy, IPsec policy template, or IPsec profile defines the parameters used for IKE negotiation.

You can specify only one IKE profile for an IPsec policy, IPsec policy template, or IPsec profile.

Examples

Specify IKE profile **profile1** for IPsec policy **policy1**.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 10 isakmp
[Sysname-ipsec-policy-isakmp-policy1-10] ike-profile profile1
```

Related commands

ike profile

ikev2-profile

Use **ikev2-profile** to specify an IKEv2 profile for an IPsec policy or IPsec policy template.

Use **undo ikev2-profile** to restore the default.

Syntax

ikev2-profile *profile-name*

undo ikev2-profile

Default

No IKEv2 profile is specified.

Views

IPsec policy view

IPsec policy template view

Predefined user roles

network-admin

Parameters

profile-name: Specifies an IKEv2 profile by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

The IKEv2 profile specified for an IPsec policy or IPsec policy template defines the parameters used for IKEv2 negotiation.

You can specify only one IKEv2 profile for an IPsec policy or IPsec policy template. On the initiator, an IKEv2 profile is required. On the responder, an IKEv2 profile is optional. If you do not specify an IKEv2 profile, the responder can use any IKEv2 profile for negotiation.

Examples

Specify IKEv2 profile **profile1** for IPsec policy **policy1**.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 10 isakmp
[Sysname-ipsec-policy-isakmp-policy1-10] ikev2-profile profile1
```

Related commands

display ipsec ipv6-policy

display ipsec policy

ikev2 profile

ipsec { ipv6-policy | policy }

Use **ipsec** { **ipv6-policy** | **policy** } to create an IPsec policy entry and enter its view, or enter the view of an existing IPsec policy entry.

Use **undo ipsec** { **ipv6-policy** | **policy** } to delete an IPsec policy.

Syntax

ipsec { **ipv6-policy** | **policy** } *policy-name seq-number* [**isakmp** | **manual**]

undo ipsec { **ipv6-policy** | **policy** } *policy-name* [*seq-number*]

Default

No IPsec policies exist.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6-policy: Specifies an IPv6 IPsec policy.

policy: Specifies an IPv4 IPsec policy.

policy-name: Specifies a name for the IPsec policy, a case-insensitive string of 1 to 63 characters.

seq-number: Specifies a sequence number for the IPsec policy entry, in the range of 1 to 65535.

isakmp: Establishes IPsec SAs through IKE negotiation.

manual: Establishes IPsec SAs manually.

Usage guidelines

When you create an IPsec policy, you must specify the SA setup mode (**isakmp** or **manual**). When you enter the view of an existing IPsec policy, you do not need to specify the SA setup mode.

You cannot change the SA setup mode of an existing IPsec policy.

An IPsec policy is a set of IPsec policy entries that have the same name but different sequence numbers. In the same IPsec policy, an IPsec policy entry with a smaller sequence number has a higher priority.

If you specify the *seq-number* argument, the **undo** command deletes the specified IPsec policy entry. If you do not specify this argument, the **undo** command deletes the specified IPsec policy.

An IPv4 IPsec policy and IPv6 IPsec policy can have the same name.

Examples

Create an IKE-based IPsec policy entry and enter the IPsec policy view. The policy name is **policy1** and the sequence number is 100.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 isakmp
[Sysname-ipsec-policy-isakmp-policy1-100]
```

Create a manual IPsec policy entry and enter the IPsec policy view. The policy name is **policy1** and the sequence number is 101.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 101 manual
[Sysname-ipsec-policy-manual-policy1-101]
```

Related commands

display ipsec { **ipv6-policy** | **policy** }

ipsec apply

ipsec { ipv6-policy | policy } isakmp template

Use **ipsec** { **ipv6-policy** | **policy** } **isakmp template** to create an IKE-based IPsec policy entry by using an IPsec policy template.

Use **undo ipsec** { **ipv6-policy** | **policy** } to delete an IPsec policy.

Syntax

ipsec { **ipv6-policy** | **policy** } *policy-name seq-number* **isakmp template** *template-name*

undo ipsec { **ipv6-policy** | **policy** } *policy-name* [*seq-number*]

Default

No IPsec policies exist.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6-policy: Specifies an IPv6 IPsec policy.

policy: Specifies an IPv4 IPsec policy.

policy-name: Specifies a name for the IPsec policy, a case-insensitive string of 1 to 63 characters.

seq-number: Specifies a sequence number for the IPsec policy, in the range of 1 to 65535. A smaller number indicates a higher priority.

isakmp template *template-name*: Specifies an IPsec policy template by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

If you specify the *seq-number* argument, the **undo** command deletes the specified IPsec policy entry. If you do not specify this argument, the **undo** command deletes the specified IPsec policy.

An interface applied with an IPsec policy that is configured by using an IPsec policy template cannot initiate an SA negotiation, but it can respond to a negotiation request. The parameters not defined in the template are determined by the initiator. When the remote end's information (such as the IP address) is unknown, this method allows the remote end to initiate negotiations with the local end.

Examples

Create an IPsec policy entry by using IPsec policy template **temp1**, and specify the IPsec policy name as **policy2** and the sequence number as 200.

```
<Sysname> system-view
[Sysname] ipsec policy policy2 200 isakmp template temp1
```

Related commands

display ipsec { **ipv6-policy** | **policy** }

ipsec { **ipv6-policy-template** | **policy-template** }

ipsec { ipv6-policy | policy } local-address

Use **ipsec** { **ipv6-policy** | **policy** } **local-address** to bind an IPsec policy to a source interface.

Use **undo ipsec** { **ipv6-policy** | **policy** } **local-address** to remove the binding between an IPsec policy and a source interface.

Syntax

ipsec { **ipv6-policy** | **policy** } *policy-name* **local-address** *interface-type interface-number*

undo ipsec { **ipv6-policy** | **policy** } *policy-name* **local-address**

Default

No IPsec policy is bound to a source interface.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6-policy: Specifies an IPv6 IPsec policy.

policy: Specifies an IPv4 IPsec policy.

policy-name: Specifies an IPsec policy name, a case-insensitive string of 1 to 63 characters.

local-address *interface-type interface-number*: Specifies the shared source interface by its type and number.

Usage guidelines

For high availability, two interfaces can operate in backup mode. After an IPsec policy is applied to the two interfaces, they negotiate with their peers to establish IPsec SAs separately. When one interface fails and a link failover occurs, the other interface needs to take some time to renegotiate SAs, resulting in service interruption.

To solve these problems, bind a source interface to an IPsec policy and apply the policy to both interfaces. This enables the two physical interfaces to use the same source interface to negotiate IPsec SAs. As long as the source interface is up, the negotiated IPsec SAs will not be removed and will keep working, regardless of link failover.

After an IPsec policy is applied to a service interface and IPsec SAs have been established, if you bind the IPsec policy to a source interface, the existing IPsec SAs are deleted.

Only an IKE-based IPsec policy can be bound to a source interface.

An IPsec policy can be bound to only one source interface. If you execute this command multiple times, the most recent configuration takes effect.

A source interface can be bound to multiple IPsec policies.

As a best practice, use a stable interface, such as a Loopback interface, as a source interface.

Examples

Bind IPsec policy **map** to source interface Loopback 11.

```
<Sysname> system-view
[Sysname] ipsec policy map local-address loopback 11
```

Related commands

ipsec { **ipv6-policy** | **policy** }

ipsec { ipv6-policy-template | policy-template }

Use **ipsec** { **ipv6-policy-template** | **policy-template** } to create an IPsec policy template entry and enter its view, or enter the view of an existing IPsec policy template entry.

Use **undo ipsec** { **ipv6-policy-template** | **policy-template** } to delete an IPsec policy template.

Syntax

ipsec { **ipv6-policy-template** | **policy-template** } *template-name seq-number*

undo ipsec { **ipv6-policy-template** | **policy-template** } *template-name* [*seq-number*]

Default

No IPsec policy templates exist.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6-policy-template: Specifies an IPv6 IPsec policy template.

policy-template: Specifies an IPv4 IPsec policy template.

template-name: Specifies a name for the IPsec policy template, a case-insensitive string of 1 to 63 characters.

seq-number: Specifies a sequence number for the IPsec policy template entry, in the range of 1 to 65535. A smaller number indicates a higher priority.

Usage guidelines

The configurable parameters for an IPsec policy template are similar to the parameters that you use when you configure an IKE-based IPsec policy. However, all parameters except for the IPsec transform sets and the IKE peer are optional for an IPsec policy template.

An IPsec policy template is a set of IPsec policy template entries that have the same name but different sequence numbers.

With the *seq-number* argument specified, the **undo** command deletes an IPsec policy template entry.

An IPv4 IPsec policy template and an IPv6 IPsec policy template can have the same name.

Examples

Create an IPsec policy template entry and enter the IPsec policy template view. The template name is **template1** and the sequence number is 100.

```
<Sysname> system-view
[Sysname] ipsec policy-template template1 100
[Sysname-ipsec-policy-template-template1-100]
```

Related commands

display ipsec { **ipv6-policy-template** | **policy-template** }

ipsec { **ipv6-policy** | **policy** }

ipsec { **ipv6-policy** | **policy** } **isakmp template**

ipsec anti-replay check

Use **ipsec anti-replay check** to enable IPsec anti-replay checking.

Use **undo ipsec anti-replay check** to disable IPsec anti-replay checking.

Syntax

ipsec anti-replay check

undo ipsec anti-replay check

Default

IPsec anti-replay checking is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

IPsec packet de-encapsulation involves complicated calculation. De-encapsulation of replayed packets is not necessary but consumes large amounts of resources and degrades performance, resulting in DoS. IPsec anti-replay checking, when enabled, is performed before the de-encapsulation process, reducing resource waste.

In some situations, service data packets are received in a different order than their original order. The IPsec anti-replay feature drops them as replayed packets, which impacts communications. If this happens, disable IPsec anti-replay checking or adjust the size of the anti-replay window as required.

Only IPsec SAs negotiated by IKE support anti-replay checking. Manually created IPsec SAs do not support anti-replay checking. Enabling or disabling IPsec anti-replay checking does not affect manually created IPsec SAs.

Examples

Enable IPsec anti-replay checking.

```
<Sysname> system-view
[Sysname] ipsec anti-replay check
```

Related commands

ipsec anti-replay window

ipsec anti-replay window

Use **ipsec anti-replay window** to set the anti-replay window size.

Use **undo ipsec anti-replay window** to restore the default.

Syntax

ipsec anti-replay window *width*

undo ipsec anti-replay window

Default

The anti-replay window size is 64.

Views

System view

Predefined user roles

network-admin

Parameters

width: Specifies the size for the anti-replay window. It can be 64, 128, 256, 512, or 1024 packets.

Usage guidelines

Service data packets might be received in a very different order than their original order, and the IPsec anti-replay feature might drop them as replayed packets, affecting normal communications. If this happens, disable IPsec anti-replay checking or adjust the size of the anti-replay window as required.

Changing the anti-replay window size affects only the IPsec SAs negotiated later.

Examples

Set the size of the anti-replay window to 128.

```
<Sysname> system-view
[Sysname] ipsec anti-replay window 128
```

Related commands

ipsec anti-replay check

ipsec apply

Use **ipsec apply** to apply an IPsec policy to an interface.

Use **undo ipsec apply** to remove an IPsec policy application from an interface.

Syntax

ipsec apply { **ipv6-policy** | **policy** } *policy-name*

undo ipsec apply { **ipv6-policy** | **policy** }

Default

No IPsec policy is applied to an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-policy: Specifies an IPv6 IPsec policy.

policy: Specifies an IPv4 IPsec policy.

policy-name: Specifies an IPsec policy name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

On an interface, you can apply a maximum of two IPsec policies: one IPv4 IPsec policy and one IPv6 IPsec policy.

An IKE-based IPsec policy can be applied to multiple interfaces. As a best practice, apply an IKE-based IPsec policy to only one interface. A manual IPsec policy can be applied to only one interface.

Examples

Apply IPsec policy **policy1** to VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname–Vlan-interface100] ipsec apply policy policy1
```

Related commands

display ipsec { **ipv6-policy** | **policy** }

ipsec { **ipv6-policy** | **policy** }

ipsec decrypt-check enable

Use **ipsec decrypt-check enable** to enable ACL checking for de-encapsulated IPsec packets.

Use **undo ipsec decrypt-check** to disable ACL checking for de-encapsulated IPsec packets.

Syntax

ipsec decrypt-check enable

undo ipsec decrypt-check enable

Default

ACL checking for de-encapsulated IPsec packets is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

In tunnel mode, the IP packet encapsulated in an inbound IPsec packet might not be under the protection of the ACL specified in the IPsec policy. After being de-encapsulated, such packets bring threats to the network security. In this scenario, you can enable ACL checking for de-encapsulated IPsec packets. All packets failing the checking are discarded, improving the network security.

Examples

Enable ACL checking for de-encapsulated IPsec packets.

```
<Sysname> system-view
[Sysname] ipsec decrypt-check enable
```

ipsec df-bit

Use **ipsec df-bit** to configure the DF bit for the outer IP header of IPsec packets on an interface.

Use **undo ipsec df-bit** to restore the default.

Syntax

ipsec df-bit { **clear** | **copy** | **set** }

undo ipsec df-bit

Default

The DF bit is not configured for the outer IP header of IPsec packets on an interface. The global DF bit setting is used.

Views

Interface view

Predefined user roles

network-admin

Parameters

clear: Clears the DF bit in the outer IP header. IPsec packets can be fragmented.

copy: Copies the DF bit setting of the original IP header to the outer IP header.

set: Sets the DF bit in the outer IP header. IPsec packets cannot be fragmented.

Usage guidelines

This command is effective only when the IPsec encapsulation mode is tunnel mode. It is not effective in transport mode because the outer IP header is not added in transport mode.

This command does not change the DF bit for the original IP header of IPsec packets.

If multiple interfaces use an IPsec policy that is bound to a source interface, you must use the same DF bit setting on these interfaces.

Packet fragmentation and reassembly might cause packet forwarding to be delayed. You can set the DF bit to avoid the forwarding delay. However, to prevent the IPsec packets from being discarded, you must make sure the path MTU is larger than the IPsec packet size. As a best practice, clear the DF bit if you cannot make sure the path MTU is larger than the IPsec packet size.

Examples

Set the DF bit in the outer IP header of IPsec packets on VLAN-interface100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname–Vlan-interface100] ipsec df-bit set
```

Related commands

ipsec global-df-bit

ipsec fragmentation

Use **ipsec fragmentation** to configure the IPsec fragmentation feature.

Use **undo ipsec fragmentation** to restore the default.

Syntax

ipsec fragmentation { **after-encryption** | **before-encryption** }

undo ipsec fragmentation

Default

The device fragments packets before IPsec encapsulation.

Views

System view

Predefined user roles

network-admin

Parameters

after-encryption: Fragments packets after IPsec encapsulation.

before-encryption: Fragments packets before IPsec encapsulation.

Usage guidelines

If you configure the device to fragment packets before IPsec encapsulation, the device predetermines the encapsulated packet size before the actual encapsulation. If the encapsulated packet size exceeds the MTU of the output interface and the DF bit is not set, the device fragments the packet before encapsulation. If the packet's DF bit is set, the device drops the packet and sends an ICMP error message.

If you configure the device to fragment packets after IPsec encapsulation, the device directly encapsulates the packets and fragments the encapsulated packets in subsequent service modules.

Examples

Configure the device to fragment packets after IPsec encapsulation.

```
<Sysname>system-view
[Sysname] ipsec fragmentation after-encryption
```

ipsec global-df-bit

Use **ipsec global-df-bit** to configure the DF bit for the outer IP header of IPsec packets on all interfaces.

Use **undo ipsec global-df-bit** to restore the default.

Syntax

ipsec global-df-bit { **clear** | **copy** | **set** }

undo ipsec global-df-bit

Default

The DF bit setting of the original IP header is copied to the outer IP header for IPsec packets.

Views

System view

Predefined user roles

network-admin

Parameters

clear: Clears the DF bit in the outer IP header. IPsec packets can be fragmented.

copy: Copies the DF bit setting of the original IP header to the outer IP header.

set: Sets the DF bit in the outer IP header. IPsec packets cannot be fragmented.

Usage guidelines

This command is effective only when the IPsec encapsulation mode is tunnel mode. It is not effective in transport mode because the outer IP header is not added in transport mode.

This command does not change the DF bit for the original IP header of IPsec packets.

Packet fragmentation and reassembly might cause packet forwarding to be delayed. You can set the DF bit to avoid the forwarding delay. However, to prevent IPsec packets from being discarded, you must make sure the path MTU is larger than the IPsec packet size. As a best practice, clear the DF bit if you cannot make sure the path MTU is larger than the IPsec packet size.

Examples

Set the DF bit in the outer IP header of IPsec packets on all interfaces.

```
<Sysname> system-view
[Sysname] ipsec global-df-bit set
```

Related commands

ipsec df-bit

ipsec limit max-tunnel

Use **ipsec limit max-tunnel** to set the maximum number of IPsec tunnels.

Use **undo ipsec limit max-tunnel** to restore the default.

Syntax

ipsec limit max-tunnel *tunnel-limit*

undo ipsec limit max-tunnel

Default

The number of IPsec tunnels is not limited.

Views

System view

Predefined user roles

network-admin

Parameters

tunnel-limit: Specifies the maximum number of IPsec tunnels, in the range of 1 to 4294967295.

Usage guidelines

To maximize concurrent performance of IPsec when memory is sufficient, increase the maximum number of IPsec tunnels. To ensure service availability when memory is insufficient, decrease the maximum number of IPsec tunnels.

Examples

Set the maximum number of IPsec tunnels to 5000.

```
<Sysname> system-view
[Sysname] ipsec limit max-tunnel 5000
```

Related commands

ike limit

ipsec logging packet enable

Use **ipsec logging packet enable** to enable logging for IPsec packets.

Use **undo ipsec logging packet enable** to disable logging for IPsec packets.

Syntax

ipsec logging packet enable

undo ipsec logging packet enable

Default

Logging for IPsec packets is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

After logging for IPsec packets is enabled, the device outputs a log when an IPsec packet is discarded. IPsec packets might be discarded due to lack of inbound SA, AH/ESP authentication failure, or ESP encryption failure. A log contains the source and destination IP addresses, SPI, and sequence number of the packet, and the reason it was discarded.

Examples

Enable logging for IPsec packets.

```
<Sysname> system-view
[Sysname] ipsec logging packet enable
```

ipsec profile

Use **ipsec profile** to create an IPsec profile and enter its view, or enter the view of an existing IPsec profile.

Use **undo ipsec profile** to delete an IPsec profile.

Syntax

ipsec profile *profile-name* [**manual**]

undo ipsec profile *profile-name*

Default

No IPsec profiles exist.

Views

System view

Predefined user roles

network-admin

Parameters

profile-name: Specifies a name for the IPsec profile, a case-insensitive string of 1 to 63 characters.

manual: Specifies the IPsec SA setup mode as manual.

Usage guidelines

When you create an IPsec profile, you must specify the IPsec SA setup mode (**manual**). When you enter the view of an existing IPsec profile, you do not need to specify the IPsec SA setup mode.

A manual IPsec profile is similar to a manual IPsec policy. It is used exclusively for IPsec protection for application protocols, including OSPFv3 and RIPng.

Examples

Create a manual IPsec profile named **profile1**.

```
<Sysname> system-view
[Sysname] ipsec profile profile1 manual
[Sysname-ipsec-profile-manual-profile1]
```

Related commands

display ipsec profile

ipsec redundancy enable

Use **ipsec redundancy enable** to enable IPsec redundancy.

Use **undo ipsec redundancy enable** to disable IPsec redundancy.

Syntax

ipsec redundancy enable

undo ipsec redundancy enable

Default

IPsec redundancy is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

With IPsec redundancy enabled, the system synchronizes the following information from the active device to the standby device at configurable intervals:

- Lower bound values of the IPsec anti-replay window for inbound packets.
- IPsec anti-replay sequence numbers for outbound packets.

The synchronization ensures uninterrupted IPsec traffic forwarding and anti-replay protection when the active device fails.

To configure synchronization intervals, use the **redundancy replay-interval** command.

Examples

Enable IPsec redundancy.

```
<Sysname> system-view
[Sysname] ipsec redundancy enable
```

Related commands

redundancy replay-interval

ipsec sa global-duration

Use **ipsec sa global-duration** to configure the global IPsec SA lifetime.

Use **undo ipsec sa global-duration** to restore the default.

Syntax

ipsec sa global-duration { **time-based** *seconds* | **traffic-based** *kilobytes* }

undo ipsec sa global-duration { **time-based** | **traffic-based** }

Default

The time-based global IPsec SA lifetime is 3600 seconds, and the traffic-based global lifetime is 1843200 kilobytes.

Views

System view

Predefined user roles

network-admin

Parameters

time-based *seconds*: Specifies the time-based global lifetime for IPsec SAs, in the range of 180 to 604800 seconds.

traffic-based *kilobytes*: Specifies the traffic-based global lifetime for IPsec SAs, in the range of 2560 to 4294967295 kilobytes. When traffic on an SA reaches this value, the SA expires.

Usage guidelines

You can also configure IPsec SA lifetimes in IPsec policy view or IPsec policy template view. The device prefers the IPsec SA lifetimes configured in IPsec policy view or IPsec policy template view over the global IPsec SA lifetimes.

When IKE negotiates IPsec SAs, it uses the local lifetime settings or those proposed by the peer, whichever are smaller.

An IPsec SA can have both a time-based lifetime and a traffic-based lifetime. The IPsec SA expires when either lifetime expires. Before the IPsec SA expires, IKE negotiates a new IPsec SA, which takes over immediately after its creation.

Examples

Configure the global IPsec SA lifetime as 7200 seconds.

```
<Sysname> system-view
[Sysname] ipsec sa global-duration time-based 7200
```

Configure the global IPsec SA lifetime as 10240 kilobytes.

```
[Sysname] ipsec sa global-duration traffic-based 10240
```

Related commands

display ipsec sa

sa duration

ipsec sa idle-time

Use **ipsec sa idle-time** to enable the global IPsec SA idle timeout feature and set the idle timeout. If no traffic matches an IPsec SA within the idle timeout interval, the IPsec SA is deleted.

Use **undo ipsec sa idle-time** to disable the global IPsec SA idle timeout feature.

Syntax

ipsec sa idle-time *seconds*

undo ipsec sa idle-time

Default

The global IPsec SA idle timeout feature is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

seconds: Specifies the IPsec SA idle timeout in the range of 60 to 86400 seconds.

Usage guidelines

This feature applies only to IPsec SAs negotiated by IKE.

The IPsec SA idle timeout can also be configured in IPsec policy view, IPsec policy template view, or IPsec profile view, which takes precedence over the global IPsec SA timeout.

Examples

Enable the global IPsec SA idle timeout feature and set the IPsec SA idle timeout to 600 seconds.

```
<Sysname> system-view
[Sysname] ipsec sa idle-time 600
```

Related commands

display ipsec sa

sa idle-time

ipsec transform-set

Use **ipsec transform-set** to create an IPsec transform set and enter its view, or enter the view of an existing IPsec transform set.

Use **undo ipsec transform-set** to delete an IPsec transform set.

Syntax

ipsec transform-set *transform-set-name*

undo ipsec transform-set *transform-set-name*

Default

No IPsec transform sets exist.

Views

System view

Predefined user roles

network-admin

Parameters

transform-set-name: Specifies a name for the IPsec transform set, a case-insensitive string of 1 to 63 characters.

Usage guidelines

An IPsec transform set, part of an IPsec policy, defines the security parameters for IPsec SA negotiation, including the security protocol, encryption algorithms, authentication algorithms, and encapsulation mode.

Examples

Create an IPsec transform set named **tran1** and enter its view.

```
<Sysname> system-view
[Sysname] ipsec transform-set tran1
[Sysname-transform-set-tran1]
```

Related commands

display ipsec transform-set

local-address

Use **local-address** to configure the local IP address for the IPsec tunnel.

Use **undo local-address** to restore the default.

Syntax

local-address { *ipv4-address* | **ipv6** *ipv6-address* }

undo local-address

Default

The primary IPv4 address of the interface to which the IPsec policy is applied is used as the local IPv4 address. The first IPv6 address of the interface to which the IPsec policy is applied is used as the local IPv6 address.

Views

IPsec policy view

IPsec policy template view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies the local IPv4 address for the IPsec tunnel.

ipv6 *ipv6-address*: Specifies the local IPv6 address for the IPsec tunnel.

Usage guidelines

The remote IP address on the IKE negotiation initiator must be the same as the local address on the IKE negotiation responder.

Examples

Configure local address 1.1.1.1 for the IPsec tunnel.

```
<Sysname> system-view
[Sysname] ipsec policy map 1 isakmp
[Sysname-ipsec-policy-isakmp-map-1] local-address 1.1.1.1
```

Related commands

remote-address

pfs

Use **pfs** to enable the Perfect Forward Secrecy (PFS) feature for an IPsec transform set.

Use **undo pfs** to restore the default.

Syntax

In non-FIPS mode:

pfs { **dh-group1** | **dh-group2** | **dh-group5** | **dh-group14** | **dh-group24** | **dh-group19** | **dh-group20** }

undo pfs

In FIPS mode:

pfs { **dh-group14** | **dh-group19** | **dh-group20** }

undo pfs

Default

The PFS feature is disabled for the IPsec transform set.

Views

IPsec transform set view

Predefined user roles

network-admin

Parameters

dh-group1: Uses 768-bit Diffie-Hellman group.

dh-group2: Uses 1024-bit Diffie-Hellman group.

dh-group5: Uses 1536-bit Diffie-Hellman group.

dh-group14: Uses 2048-bit Diffie-Hellman group.

dh-group24: Uses 2048-bit and 256-bit subgroup Diffie-Hellman group.

dh-group19: Uses 256-bit ECP Diffie-Hellman group. This keyword is available only for IKEv2.

dh-group20: Uses 384-bit ECP Diffie-Hellman group. This keyword is available only for IKEv2.

Usage guidelines

In terms of security and required calculation time, the following groups are in descending order: 384-bit ECP Diffie-Hellman group (**dh-group20**), 256-bit ECP Diffie-Hellman group (**dh-group19**), 2048-bit and 256-bit subgroup Diffie-Hellman group (**dh-group24**), 2048-bit Diffie-Hellman group (**dh-group14**), 1536-bit Diffie-Hellman group (**dh-group5**), 1024-bit Diffie-Hellman group (**dh-group2**), and 768-bit Diffie-Hellman group (**dh-group1**).

If IKEv1 is used, the security level of the Diffie-Hellman group of the initiator must be higher than or equal to that of the responder. This restriction does not apply to IKEv2.

The end without the PFS feature performs IKE negotiation according to the PFS requirements of the peer end.

Examples

Enable PFS using 2048-bit Diffie-Hellman group for IPsec transform set **tran1**.

```
<Sysname> system-view
[Sysname] ipsec transform-set tran1
[Sysname-ipsec-transform-set-tran1] pfs dh-group14
```

protocol

Use **protocol** to specify a security protocol for an IPsec transform set.

Use **undo protocol** to restore the default.

Syntax

protocol { **ah** | **ah-esp** | **esp** }

undo protocol

Default

The IPsec transform set uses the ESP protocol.

Views

IPsec transform set view

Predefined user roles

network-admin

Parameters

ah: Specifies the AH protocol.

ah-esp: Specifies using the ESP protocol first and then using the AH protocol.

ah: Specifies the AH protocol.

Usage guidelines

The two tunnel ends must use the same security protocol in the IPsec transform set.

Examples

Specify the AH protocol for the IPsec transform set.

```
<Sysname> system-view
[Sysname] ipsec transform-set tran1
[Sysname-ipsec-transform-set-tran1] protocol ah
```

qos pre-classify

Use **qos pre-classify** to enable the QoS pre-classify feature.

Use **undo qos pre-classify** to disable the QoS pre-classify feature.

Syntax

qos pre-classify

undo qos pre-classify

Default

The QoS pre-classify feature is disabled. QoS uses the new IP header of IPsec packets to perform traffic classification.

Views

IPsec policy view

IPsec policy template view

Predefined user roles

network-admin

Usage guidelines

The QoS pre-classify feature enables QoS to classify packets by using the IP header of the original IP packets.

Examples

Enable the QoS pre-classify feature.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] qos pre-classify
```

redundancy replay-interval

Use **redundancy replay-interval** to set the anti-replay window lower bound value synchronization interval for inbound packets and the sequence number synchronization interval for outbound packets.

Use **undo redundancy replay-interval** to restore the default.

Syntax

redundancy replay-interval inbound *inbound-interval* **outbound** *outbound-interval*

undo redundancy replay-interval

Default

The active device synchronizes the anti-replay window lower bound value every time it receives 1000 packets and synchronizes the sequence number every time it sends 100000 packets.

Views

IPsec policy view

IPsec policy template view

Predefined user roles

network-admin

Parameters

inbound *inbound-interval*: Specifies the interval at which the active device synchronizes the lower bound value of the IPsec anti-replay window to the standby device. This interval is expressed in the number of received packets, in the range of 0 to 1000. If you set the value to 0, the lower bound value of the anti-replay window will not be synchronized.

outbound *outbound-interval*: Specifies the interval at which the active device synchronizes the IPsec anti-replay sequence number to the standby device. This interval is expressed in the number of sent packets, in the range of 1000 to 100000.

Usage guidelines

The intervals take effect only after you enable IPsec redundancy by using the **ipsec redundancy enable** command.

A short interval improves the anti-replay information consistency between the active device and the standby device, but it sacrifices the forwarding performance of the devices.

Examples

Set the anti-replay window lower bound value synchronization interval for inbound packets to 800. Set the sequence number synchronization interval for outbound packets to 50000.

```
<Sysname> system-view
[Sysname] ipsec policy test 1 manual
[sysname-ipsec-policy-manual-test-1] redundancy replay-interval inbound 800 outbound
50000
```

Related commands

ipsec anti-replay check

ipsec anti-replay window

ipsec redundancy enable

remote-address

Use **remote-address** to configure the remote IP address for the IPsec tunnel.

Use **undo remote-address** to restore the default.

Syntax

remote-address { [**ipv6**] *host-name* | *ipv4-address* | **ipv6** *ipv6-address* }

undo remote-address

Default

No remote IP address is configured for the IPsec tunnel.

Views

IPsec policy view

IPsec policy template view

Predefined user roles

network-admin

Parameters

ipv6: Specifies the remote address or host name of an IPv6 IPsec tunnel. To specify the remote address or host name of an IPv4 IPsec tunnel, do not specify this keyword.

hostname: Specifies the remote host name, a case-insensitive string of 1 to 253 characters. The host name can be resolved to an IP address by the DNS server.

ipv4-address: Specifies a remote IPv4 address.

ipv6-address: Specifies a remote IPv6 address.

Usage guidelines

This remote IP address configuration is required on the IKE negotiation initiator and optional on the responder if the responder uses an IPsec policy template.

A manual IPsec policy does not support DNS. Therefore, you must specify a remote IP address rather than a remote host name for the manual IPsec policy.

If you configure a remote host name, make sure the local end can always resolve the host name into the latest IP address of the remote end.

- If a DNS server is used for resolution, the local end queries the remote IP address again from the DNS server after the previously cached remote IP address expires. This mechanism ensures that the local end can always obtain the latest remote IP address.
- If a static DNS entry is used for resolution, you must reconfigure the **remote-address** command whenever the remote IP address changes. Without the reconfiguration, the local end cannot obtain the latest remote IP address.

For example, the local end has a static DNS entry which maps the host name **test** to the IP address 1.1.1.1. Configure the following commands:

Configure the remote host name to **test** for the IPsec tunnel in the IPsec policy **policy1**.

```
[Sysname] ipsec policy policy1 1 isakmp
[Sysname-ipsec-policy-isakmp-policy1-1] remote-address test
```

Change the IP address for the host **test** to 2.2.2.2.

```
[Sysname] ip host test 2.2.2.2
```

In this case, you must reconfigure the remote host name for the IPsec policy **policy1** so that the local end can obtain the latest IP address of the remote host.

Reconfigure the remote host name to **test** for the IPsec tunnel in the IPsec policy **policy1**.

```
[Sysname] ipsec policy policy1 1 isakmp
[Sysname -ipsec-policy-isakmp-policy1-1] remote-address test
```

Examples

Specify remote IP address 10.1.1.2 for the IPsec tunnel.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 10 manual
[Sysname-ipsec-policy-manual-policy1-10] remote-address 10.1.1.2
```

Related commands

ip host (*Layer 3—IP Services Command Reference*)

local-address

reset ipsec sa

Use **reset ipsec sa** to clear IPsec SAs.

Syntax

reset ipsec sa [{ **ipv6-policy** | **policy** } *policy-name* [*seq-number*] | **profile** *policy-name* | **remote** { *ipv4-address* | **ipv6** *ipv6-address* } | **spi** { *ipv4-address* | **ipv6** *ipv6-address* } { **ah** | **esp** } *spi-num*]

Views

User view

Predefined user roles

network-admin

Parameters

{ **ipv6-policy** | **policy** } *policy-name* [*seq-number*]: Clears IPsec SAs for the specified IPsec policy.

- **ipv6-policy**: Specifies an IPv6 IPsec policy.
- **policy**: Specifies an IPv4 IPsec policy.
- *policy-name*: Specifies the name of the IPsec policy, a case-insensitive string of 1 to 63 characters.
- *seq-number*: Specifies the sequence number of an IPsec policy entry, in the range of 1 to 65535. If you do not specify this argument, all the entries in the IPsec policy are specified.

profile *profile-name*: Clears IPsec SAs for the IPsec profile specified by its name, a case-insensitive string of 1 to 63 characters.

remote: Clears IPsec SAs for the specified remote address.

ipv4-address: Specifies a remote IPv4 address.

ipv6 *ipv6-address*: Specifies a remote IPv6 address.

spi { *ipv4-address* | **ipv6** *ipv6-address* } { **ah** | **esp** } *spi-num*: Clears IPsec SAs matching the specified SA triplet: the remote address, the security protocol, and the SPI.

- *ipv4-address*: Specifies a remote IPv4 address.
- **ipv6** *ipv6-address*: Specifies a remote IPv6 address.
- **ah**: Specifies the AH protocol.
- **esp**: Specifies the ESP protocol.

spi-num: Specifies the security parameter index in the range of 256 to 4294967295.

Usage guidelines

If you do not specify any parameters, this command clears all IPsec SAs.

If you specify an SA triplet, this command clears the IPsec SA matching the triplet, and all the other IPsec SAs that were established during the same negotiation process, including the corresponding IPsec SA in the other direction, and the inbound and outbound IPsec SAs using the other security protocol (AH or ESP).

An outbound SA is uniquely identified by an SA triplet and an inbound SA is uniquely identified by an SPI. To clear IPsec SAs by specifying a triplet in the outbound direction, you should provide the remote IP address, the security protocol, and the SPI, where the remote IP address can be any valid

address if the SAs are established by IPsec profiles. To clear IPsec SAs by specifying a triplet in the inbound direction, you should provide the SPI and use any valid values for the other two parameters.

After a manual IPsec SA is cleared, the system automatically creates a new SA based on the parameters of the IPsec policy. After IKE negotiated SAs are cleared, the system creates new SAs only when IKE negotiation is triggered by packets.

Examples

Clear all IPsec SAs.

```
<Sysname> reset ipsec sa
```

Clear the inbound and outbound IPsec SAs for the triplet of SPI 256, remote IP address 10.1.1.2, and security protocol AH.

```
<Sysname> reset ipsec sa spi 10.1.1.2 ah 256
```

Clear all IPsec SAs for remote IP address 10.1.1.2.

```
<Sysname> reset ipsec sa remote 10.1.1.2
```

Clear all IPsec SAs for entry 10 of IPsec policy **policy1**.

```
<Sysname> reset ipsec sa policy policy1 10
```

Clear all IPsec SAs for IPsec policy **policy1**.

```
<Sysname> reset ipsec sa policy policy1
```

Related commands

display ipsec sa

reset ipsec statistics

Use **reset ipsec statistics** to clear IPsec packet statistics.

Syntax

reset ipsec statistics[**tunnel-id** *tunnel-id*]

Views

User view

Predefined user roles

network-admin

Parameters

tunnel-id *tunnel-id*: Clears IPsec packet statistics for the specified IPsec tunnel. The value range for the *tunnel-id* argument is 0 to 4294967295. If you do not specify this option, the command clears all IPsec packet statistics.

Examples

Clear IPsec packet statistics.

```
<Sysname> reset ipsec statistics
```

Related commands

display ipsec statistics

reverse-route dynamic

Use **reverse-route dynamic** to enable IPsec reverse route inject (RRI).

Use **undo reverse-route dynamic** to disable IPsec RRI.

Syntax

reverse-route dynamic

undo reverse-route dynamic

Default

IPsec RRI is disabled.

Views

IPsec policy view

IPsec policy template view

Predefined user roles

network-admin

Usage guidelines

IPsec RRI is usually used on a gateway device at the headquarters side in an IPsec VPN. After IPsec RRI is enabled for an IPsec policy or an IPsec policy template on a gateway device, the gateway device automatically creates a static route upon IPsec SA creation according to this IPsec policy or IPsec policy template. In the static route, the destination IP address is the protected peer private network, and the next hop is the IP address of the remote tunnel interface.

When you enable IPsec RRI for an IPsec policy, the device deletes all IPsec SAs that are created according to this IPsec policy. Upon IPsec SAs are renegotiated, the static routes are created.

When you disable IPsec RRI for an IPsec policy, the device deletes all IPsec SAs that are created according to this IPsec policy, and the associated static routes.

To display the static routes created by RRI, use the **display ip routing-table** command.

Examples

Enable IPsec RRI to create a static route according to the IPsec SA negotiated by the specified IPsec policy. The destination IP address is the protected peer private network 3.0.0.0/24, and the next hop is the IP address (1.1.1.2) of the remote tunnel interface.

```
<Sysname> system-view
[Sysname] ipsec policy 1 1 isakmp
[Sysname-ipsec-policy-isakmp-1-1] reverse-route dynamic
[Sysname-ipsec-policy-isakmp-1-1] quit
```

Display the routing table. You can see a created static route. (Other information is not shown.)

```
[Sysname] display ip routing-table

Destinations : 1        Routes : 1

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
3.0.0.0/24          Static 60   0            1.1.1.2         Vlan100
```

Related commands

display ip routing-table (*Layer 3—IP Routing Command Reference)*

ipsec policy

ipsec policy-template

reverse-route preference

Use **reverse-route preference** to set the preference of the static routes created by IPsec RRI.

Use **undo reverse-route preference** to restore the default.

Syntax

reverse-route preference *number*

undo reverse-route preference

Default

The preference for the static routes created by IPsec RRI is 60.

Views

IPsec policy view

IPsec policy template view

Predefined user roles

network-admin

Parameters

number: Specifies a preference value. The value range is 1 to 255. A smaller value represents a higher preference.

Usage guidelines

When you change this preference in an IPsec policy, the device deletes all IPsec SAs created according to this IPsec policy, and the associated static routes.

Examples

Change the preference to 100 for static routes created by IPsec RRI.

```
<Sysname> system-view
[Sysname] ipsec policy 1 1 isakmp
[Sysname-ipsec-policy-isakmp-1-1] reverse-route preference 100
```

Related commands

ipsec policy

ipsec policy-template

reverse-route tag

Use **reverse-route tag** to set a route tag for the static routes created by IPsec RRI.

Use **undo reverse-route tag** to restore the default.

Syntax

reverse-route tag *tag-value*

undo reverse-route tag

Default

The route tag value is 0 for the static routes created by IPsec RRI.

Views

IPsec policy view

IPsec policy template view

Predefined user roles

network-admin

Parameters

tag-value: Specifies a tag value. The value range is 1 to 4294967295.

Usage guidelines

The tag value set by this command helps in implementing flexible route control through routing policies.

When you change this tag value in an IPsec policy, the device deletes all IPsec SAs created by this IPsec policy, and all associated static routes.

Examples

Set the tag value to 50 for the static routes created by IPsec RRI.

```
<Sysname>system-view
[Sysname] ipsec policy 1 1 isakmp
[Sysname-ipsec-policy-isakmp-1-1] reverse-route tag 50
```

Related commands

ipsec policy

ipsec policy-template

sa duration

Use **sa duration** to set an SA lifetime.

Use **undo sa duration** to remove an SA lifetime.

Syntax

sa duration { **time-based** *seconds* | **traffic-based** *kilobytes* }

undo sa duration { **time-based** | **traffic-based** }

Default

The SA lifetime of an IPsec policy, IPsec policy template, or IPsec profile is the current global SA lifetime.

Views

IPsec policy view

IPsec policy template view

IPsec profile view

Predefined user roles

network-admin

Parameters

time-based *seconds*: Specifies the time-based SA lifetime in the range of 180 to 604800 seconds.

traffic-based *kilobytes*: Specifies the traffic-based SA lifetime in the range of 2560 to 4294967295 kilobytes.

Usage guidelines

IKE prefers the SA lifetime of the IPsec policy, IPsec policy template, or IPsec profile over the global SA lifetime configured by the **ipsec sa global-duration** command. If the IPsec policy, IPsec policy template, or IPsec profile is not configured with the SA lifetime, IKE uses the global SA lifetime for SA negotiation.

During SA negotiation, IKE selects the shorter SA lifetime between the local SA lifetime and the remote SA lifetime.

Examples

Set the SA lifetime to 7200 seconds for IPsec policy **policy1**.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 isakmp
[Sysname-ipsec-policy-isakmp-policy1-100] sa duration time-based 7200
```

Set the SA lifetime to 20 MB for IPsec policy **policy1**. The IPsec SA expires after transmitting 20480 kilobytes.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 isakmp
[Sysname-ipsec-policy-isakmp-policy1-100] sa duration traffic-based 20480
```

Related commands

display ipsec sa

ipsec sa global-duration

sa hex-key authentication

Use **sa hex-key authentication** to configure an authentication key for a manual IPsec SA.

Use **undo sa hex-key authentication** to delete an authentication key for a manual IPsec SA.

Syntax

sa hex-key authentication { **inbound** | **outbound** } { **ah** | **esp** } { **cipher** | **simple** } *string*

undo sa hex-key authentication { **inbound** | **outbound** } { **ah** | **esp** }

Default

No hexadecimal authentication keys are configured for manual IPsec SAs.

Views

IPsec policy view

IPsec profile view

Predefined user roles

network-admin

Parameters

inbound: Specifies a hexadecimal authentication key for the inbound SA.

outbound: Specifies a hexadecimal authentication key for the outbound SA.

ah: Uses AH.

esp: Uses ESP.

cipher: Specifies a key in encrypted form.

simple: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. Its plaintext form is case insensitive and must be a 16-byte hexadecimal string for HMAC-MD5 and a 20-byte hexadecimal string for HMAC-SHA1. Its encrypted form is a case-sensitive string of 1 to 85 characters.

Usage guidelines

This command applies only to manual IPsec policies and IPsec profiles.

You must set an authentication key for both the inbound and outbound SAs.

The local inbound SA must use the same authentication key as the remote outbound SA, and the local outbound SA must use the same authentication key as the remote inbound SA.

In an IPsec profile to be applied to an IPv6 routing protocol, the local authentication keys of the inbound and outbound SAs must be identical.

The keys for the IPsec SAs at the two tunnel ends must be input in the same format (either in hexadecimal or character format). Otherwise, they cannot establish an IPsec tunnel.

If you execute this command multiple times for the same protocol and direction, the most recent configuration takes effect.

Examples

Configure plaintext authentication keys **0x112233445566778899aabbccddeeff00** and **0xaabbccddeeff001100aabbccddeeff00** for the inbound and outbound SAs that use AH.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] sa hex-key authentication inbound ah simple
112233445566778899aabbccddeeff00
[Sysname-ipsec-policy-manual-policy1-100] sa hex-key authentication outbound ah simple
aabbccddeeff001100aabbccddeeff00
```

Related commands

display ipsec sa

sa string-key

sa hex-key encryption

Use **sa encryption-hex** to configure an encryption key for a manual IPsec SA.

Use **undo sa encryption-hex** to delete an encryption key for a manual IPsec SA.

Syntax

sa hex-key encryption { **inbound** | **outbound** } **esp** { **cipher** | **simple** } *string*

undo sa hex-key encryption { **inbound** | **outbound** } **esp**

Default

No hexadecimal encryption keys are configured for manual IPsec SAs.

Views

IPsec policy view

IPsec profile view

Predefined user roles

network-admin

Parameters

inbound: Specifies a hexadecimal encryption key for the inbound SA.

outbound: Specifies a hexadecimal encryption key for the outbound SA.

esp: Uses ESP.

cipher: Specifies a key in encrypted form.

simple: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. Its encrypted form is a case-sensitive string of 1 to 117 characters. Its plaintext form is a case-insensitive hexadecimal string and the key length varies by algorithm.

The following matrix shows the key length for the algorithms:

Algorithm	Key length (bytes)
DES-CBC	8
3DES-CBC	24
AES128-CBC	16
AES192-CBC	24
AES256-CBC	32

Usage guidelines

This command applies only to manual IPsec policies and IPsec profiles.

You must set an encryption key for both the inbound and outbound SAs.

The local inbound SA must use the same encryption key as the remote outbound SA, and the local outbound SA must use the same encryption key as the remote inbound SA.

In an IPsec profile to be applied to an IPv6 routing protocol, the local encryption keys of the inbound and outbound SAs must be identical.

The keys for the IPsec SAs at the two tunnel ends must be configured in the same format (either in hexadecimal or character format). Otherwise, they cannot establish an IPsec tunnel.

If you execute this command multiple times for the same direction, the most recent configuration takes effect.

Examples

Configure plaintext encryption keys **0x1234567890abcdef** and **0xabcdefabcdef1234** for the inbound and outbound IPsec SAs that use ESP.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] sa hex-key encryption inbound esp simple
1234567890abcdef
[Sysname-ipsec-policy-manual-policy1-100] sa hex-key encryption outbound esp simple
abcdefabcdef1234
```

Related commands

display ipsec sa

sa string-key

sa idle-time

Use **sa idle-time** to set the IPsec SA idle timeout. If no traffic matches an IPsec SA within the idle timeout interval, the IPsec SA is deleted.

Use **undo sa idle-time** to restore the default.

Syntax

sa idle-time *seconds*

undo sa idle-time

Default

An IPsec policy, IPsec policy template, or IPsec profile uses the global IPsec SA idle timeout.

Views

IPsec policy view

IPsec policy template view

IPsec profile view

Predefined user roles

network-admin

Parameters

seconds: Specifies the IPsec SA idle timeout in the range of 60 to 86400 seconds.

Usage guidelines

This feature applies only to IPsec SAs negotiated by IKE and takes effect after the **ipsec sa idle-time** command is configured.

The IPsec SA idle timeout configured by this command takes precedence over the global IPsec SA timeout configured by the **ipsec sa idle-time** command. If the IPsec policy, IPsec policy template, or IPsec profile is not configured with the SA idle timeout, IKE uses the global SA idle timeout.

Examples

Set the IPsec SA idle timeout to 600 seconds for IPsec policy **map**.

```
<Sysname> system-view
[Sysname] ipsec policy map 100 isakmp
[Sysname-ipsec-policy-isakmp-map-100] sa idle-time 600
```

Related commands

display ipsec sa

ipsec sa idle-time

sa spi

Use **sa spi** to configure an SPI for IPsec SAs.

Use **undo sa spi** to remove the SPI.

Syntax

sa spi { **inbound** | **outbound** } { **ah** | **esp** } *spi-number*

undo sa spi { **inbound** | **outbound** } { **ah** | **esp** }

Default

No SPI is configured for IPsec SAs.

Views

IPsec policy view

IPsec profile view

Predefined user roles

network-admin

Parameters

inbound: Specifies an SPI for inbound SAs.

outbound: Specifies an SPI for outbound SAs.

ah: Uses AH.

esp: Uses ESP.

spi-number: Specifies a security parameters index (SPI) in the range of 256 to 4294967295.

Usage guidelines

This command applies only to manual IPsec policies and IPsec profiles.

You must configure an SPI for both inbound and outbound SAs, and make sure the SAs in each direction are unique: For an outbound SA, make sure its triplet (remote IP address, security protocol, and SPI) is unique. For an inbound SA, make sure its SPI is unique.

The local inbound SA must use the same SPI as the remote outbound SA, and the local outbound SA must use the same SPI as the remote inbound SA.

When you configure an IPsec profile for an IPv6 routing protocol, follow these guidelines:

- The local inbound and outbound SAs must use the same SPI.
- The IPsec SAs on the devices in the same scope must have the same SPI. The scope is defined by protocols. For OSPFv3, the scope consists of OSPFv3 neighbors or an OSPFv3 area. For RIPng, the scope consists of directly-connected neighbors or a RIPng process.

Examples

Set the SPI for the inbound SA to 10000 and the SPI for the outbound SA to 20000 in a manual IPsec policy.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] sa spi inbound ah 10000
[Sysname-ipsec-policy-manual-policy1-100] sa spi outbound ah 20000
```

Related commands

display ipsec sa

sa string-key

Use **sa string-key** to set a key string (a key in character format) for manual IPsec SAs.

Use **undo sa string-key** to remove the key string.

Syntax

sa string-key { **inbound** | **outbound** } { **ah** | **esp** } [**cipher** | **simple**] *string*

undo sa string-key { **inbound** | **outbound** } { **ah** | **esp** }

Default

No key string is configured for manual IPsec SAs.

Views

IPsec policy view

IPsec profile view

Predefined user roles

network-admin

Parameters

inbound: Sets a key string for inbound IPsec SAs.

outbound: Sets a key string for outbound IPsec SAs.

ah: Uses AH.

esp: Uses ESP.

cipher: Specifies a key string in encrypted form.

simple: Specifies a key string in plaintext form. For security purposes, the key string specified in plaintext form will be stored in encrypted form.

string: Specifies the key string. Its encrypted form is a case-sensitive string of 1 to 373 characters. Its plaintext form is a case-sensitive string of 1 to 255 characters. Using the key string, the system automatically generates keys that meet the algorithm requirements. When the protocol is ESP, the system automatically generates keys for the authentication algorithm and encryption algorithm.

Usage guidelines

This command applies only to manual IPsec policies and IPsec profiles.

You must set a key for both inbound and outbound SAs.

The local inbound SA must use the same key as the remote outbound SA, and the local outbound SA must use the same key as the remote inbound SA.

The keys for the IPsec SAs at the two tunnel ends must be input in the same format (either in hexadecimal or character format). Otherwise, they cannot establish an IPsec tunnel.

When you configure an IPsec profile for an IPv6 routing protocol, follow these guidelines:

- The local inbound and outbound SAs must use the same key.
- The IPsec SAs on the devices in the same scope must have the same key. The scope is defined by protocols. For OSPFv3, the scope consists of OSPFv3 neighbors or an OSPFv3 area. For RIPng, the scope consists of directly-connected neighbors or a RIPng process.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure the inbound and outbound SAs that use AH to use plaintext keys **abcdef** and **efcdab**, respectively.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] sa string-key inbound ah simple abcdef
[Sysname-ipsec-policy-manual-policy1-100] sa string-key outbound ah simple efcdab
```

In an IPv6 IPsec policy, configure the inbound and outbound SAs that use AH to use plaintext key **abcdef**.

```
<Sysname> system-view
[Sysname] ipsec ipv6-policy policy1 100 manual
```

```
[Sysname-ipsec-ipv6-policy-manual-policy1-100] sa string-key inbound ah simple abcdef
[Sysname-ipsec-ipv6-policy-manual-policy1-100] sa string-key outbound ah simple abcdef
```

Related commands

display ipsec sa

sa hex-key

security acl

Use **security acl** to specify an ACL for an IPsec policy or IPsec policy template.

Use **undo security acl** to restore the default.

Syntax

security acl [**ipv6**] { *acl-number* | **name** *acl-name* } [**aggregation** | **per-host**]

undo security acl

Default

An IPsec policy or IPsec policy template does not use any ACL.

Views

IPsec policy view

IPsec policy template view

Predefined user roles

network-admin

Parameters

ipv6: Specifies an IPv6 ACL.

acl-number: Specifies an ACL by its number in the range of 3000 to 3999.

name *acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters.

aggregation: Specifies the data protection mode as aggregation. The device does not support protecting IPv6 data flows in aggregation mode.

per-host: Specifies the data protection mode as per-host.

Usage guidelines

An IKE-based IPsec policy supports the following data flow protection modes:

- **Standard mode**—One IPsec tunnel protects one data flow. The data flow permitted by an ACL rule is protected by one IPsec tunnel that is established solely for it. The standard mode is used if you do not specify the aggregation or the per-host mode.
- **Aggregation mode**—One IPsec tunnel protects all data flows permitted by all the rules of an ACL. This mode is only used to communicate with old-version devices.
- **Per-host mode**—One IPsec tunnel protects one host-to-host data flow. One host-to-host data flow is identified by one ACL rule and protected by one IPsec tunnel established solely for it. This mode consumes more system resources when multiple data flows exist between two subnets to be protected.

A manual IPsec policy supports only the aggregation mode.

Examples

Specify IPv4 advanced ACL 3001 for IPsec policy **policy1**.

```
<Sysname> system-view
[Sysname] acl advanced 3001
[Sysname-acl-ipv4-adv-3001] rule permit tcp source 10.1.1.0 0.0.0.255 destination
10.1.2.0 0.0.0.255
[Sysname-acl-ipv4-adv-3001] quit
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] security acl 3001
```

Specify IPv4 advanced ACL 3002 for IPsec policy **policy2** and specify the data protection mode as aggregation.

```
<Sysname> system-view
[Sysname] acl advanced 3002
[Sysname-acl-ipv4-adv-3002] rule 0 permit ip source 10.1.2.1 0.0.0.255 destination
10.1.2.2 0.0.0.255
[Sysname-acl-ipv4-adv-3002] rule 1 permit ip source 10.1.3.1 0.0.0.255 destination
10.1.3.2 0.0.0.255
[Sysname-acl-ipv4-adv-3002] quit
[Sysname] ipsec policy policy2 1 isakmp
[Sysname-ipsec-policy-isakmp-policy2-1] security acl 3002 aggregation
```

Related commands

display ipsec sa

display ipsec tunnel

snmp-agent trap enable ipsec

Use **snmp-agent trap enable ipsec** command to enable SNMP notifications for IPsec.

Use **undo snmp-agent trap enable ipsec** command to disable SNMP notifications for IPsec.

Syntax

snmp-agent trap enable ipsec [**auth-failure** | **decrypt-failure** | **encrypt-failure** | **global** | **invalid-sa-failure** | **no-sa-failure** | **policy-add** | **policy-attach** | **policy-delete** | **policy-detach** | **tunnel-start** | **tunnel-stop**] *

undo snmp-agent trap enable ipsec [**auth-failure** | **decrypt-failure** | **encrypt-failure** | **global** | **invalid-sa-failure** | **no-sa-failure** | **policy-add** | **policy-attach** | **policy-delete** | **policy-detach** | **tunnel-start** | **tunnel-stop**] *

Default

All SNMP notifications for IPsec are disabled.

Views

System view

Predefined user roles

network-admin

Parameters

auth-failure: Specifies notifications about authentication failures.

decrypt-failure: Specifies notifications about decryption failures.

encrypt-failure: Specifies notifications about encryption failures.

global: Specifies notifications globally.

invalid-sa-failure: Specifies notifications about invalid-SA failures.

no-sa-failure: Specifies notifications about SA-not-found failures.

policy-add: Specifies notifications about events of adding IPsec policies.

policy-attach: Specifies notifications about events of applying IPsec policies to interfaces.

policy-delete: Specifies notifications about events of deleting IPsec policies.

policy-detach: Specifies notifications about events of removing IPsec policies from interfaces.

tunnel-start: Specifies notifications about events of creating IPsec tunnels.

tunnel-stop: Specifies notifications about events of deleting IPsec tunnels.

Usage guidelines

If you do not specify any keywords, this command enables or disables all SNMP notifications for IPsec.

To generate and output SNMP notifications for a specific IPsec failure type or event type, perform the following tasks:

1. Enable SNMP notifications for IPsec globally.
2. Enable SNMP notifications for the failure type or event type.

Examples

Enable SNMP notifications for IPsec globally.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable ipsec global
```

Enable SNMP notifications for events of creating IPsec tunnels.

```
[Sysname] snmp-agent trap enable ipsec tunnel-start
```

tfc enable

Use **tfc enable** to enable Traffic Flow Confidentiality (TFC) padding.

Use **undo tfc enable** to disable TFC padding.

Syntax

tfc enable

undo tfc enable

Default

TFC padding is disabled.

Views

IPsec policy view

IPsec policy template view

Predefined user roles

network-admin

Usage guidelines

TFC padding can hide the length of the original packet, and might affect the packet encapsulation and de-encapsulation performance. This feature takes effect on UDP packets encapsulated by ESP in transport mode and on original IP packets encapsulated by ESP in tunnel mode.

Examples

Enable TFC padding for IPsec policy **policy1**.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 10 isakmp
[Sysname-ipsec-policy-isakmp-policy1-10] tfc enable
```

Related commands

display ipsec ipv6-policy

display ipsec policy

transform-set

Use **transform-set** to specify an IPsec transform set for an IPsec policy, IPsec policy template, or IPsec profile.

Use **undo transform-set** to remove the IPsec transform set specified for an IPsec policy, IPsec policy template, or IPsec profile.

Syntax

transform-set *transform-set-name*&<1-6>

undo transform-set [*transform-set-name*]

Default

No IPsec transform set is specified for an IPsec policy, IPsec policy template, or IPsec profile.

Views

IPsec policy view

IPsec policy template view

IPsec profile view

Predefined user roles

network-admin

Parameters

transform-set-name&<1-6>: Specifies a space-separated list of up to six IPsec transform sets by their names, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can specify only one IPsec transform set for a manual IPsec policy. If you execute this command multiple times, the most recent configuration takes effect.

You can specify a maximum of six IPsec transform sets for an IKE-based IPsec policy. During an IKE negotiation, IKE searches for a fully matched IPsec transform set at the two ends of the IPsec tunnel. If no match is found, no SA can be set up, and the packets expecting to be protected will be dropped.

If you do not specify the *transform-set-name* argument, the **undo transform-set** command removes all IPsec transform sets specified for the IPsec policy, IPsec policy template, or IPsec profile.

Examples

Specify IPsec transform set **prop1** for IPsec policy **policy1**.

```
<Sysname> system-view
[Sysname] ipsec transform-set prop1
[Sysname-ipsec-transform-set-prop1] quit
```

```
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] transform-set prop1
```

Related commands

ipsec { **ipv6-policy** | **policy** }

ipsec profile

ipsec transform-set

IKE commands

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

authentication-algorithm

Use **authentication-algorithm** to specify an authentication algorithm for an IKE proposal.

Use **undo authentication-algorithm** to restore the default.

Syntax

In non-FIPS mode:

authentication-algorithm { **md5** | **sha** | **sha256** | **sha384** | **sha512** }

undo authentication-algorithm

In FIPS mode:

authentication-algorithm { **sha**| **sha256** | **sha384** | **sha512** }

undo authentication-algorithm

Default

In non-FIPS mode:

The IKE proposal uses the HMAC-SHA1 authentication algorithm.

In FIPS mode:

The IKE proposal uses the HMAC-SHA256 authentication algorithm.

Views

IKE proposal view

Predefined user roles

network-admin

Parameters

md5: Specifies the HMAC-MD5 algorithm.

sha: Specifies the HMAC-SHA1 algorithm.

sha256: Specifies the HMAC-SHA256 algorithm.

sha384: Specifies the HMAC-SHA384 algorithm.

sha512: Specifies the HMAC-SHA512 algorithm.

Examples

Specify HMAC-SHA1 as the authentication algorithm for IKE proposal 1.

```
<Sysname> system-view
[Sysname] ike proposal 1
[Sysname-ike-proposal-1] authentication-algorithm sha
```

Related commands

display ike proposal

authentication-method

Use **authentication-method** to specify an authentication method to be used in an IKE proposal.

Use **undo authentication-method** to restore the default.

Syntax

authentication-method { **dsa-signature** | **ecdsa-signature** | **pre-share** | **rsa-signature** }

undo authentication-method

Default

The IKE proposal uses the preshared key authentication method.

Views

IKE proposal view

Predefined user roles

network-admin

Parameters

dsa-signature: Specifies the DSA signature authentication method.

ecdsa-signature: Specifies the ECDSA signature authentication method.

pre-share: Specifies the preshared key authentication method.

rsa-signature: Specifies the RSA signature authentication method.

Usage guidelines

Preshared key authentication does not require certificates as signature authentication does, and it is usually used in a simple network. Signature authentication provides higher security, and it is usually deployed in a large-scale network, such as a network with many branches. In a network with many branches, using preshared key authentication requires the headquarters to configure a preshared key for each branch. Using signature authentication only requires the headquarters to configure one PKI domain.

Authentication methods configured on both IKE ends must match.

To use the RSA, DSA, or ECDSA signature authentication method, make sure the IKE peer can obtain certificates from a CA.

If you specify the preshared key authentication method, you must configure the preshared key on both IKE ends.

Examples

Specify the preshared key authentication method for IKE proposal 1.

```
<Sysname> system-view
[Sysname] ike proposal 1
[Sysname-ike-proposal-1] authentication-method pre-share
```

Related commands

display ike proposal

ike keychain

pre-shared-key

certificate domain

Use **certificate domain** to specify a PKI domain for signature authentication.

Use **undo certificate domain** to remove a PKI domain for signature authentication.

Syntax

certificate domain *domain-name*

undo certificate domain *domain-name*

Default

No PKI domains are specified for signature authentication.

Views

IKE profile view

Predefined user roles

network-admin

Parameters

domain-name: Specifies the name of a PKI domain, a case-insensitive string of 1 to 31 characters.

Usage guidelines

You can specify a maximum of six PKI domains for an IKE profile by executing this command multiple times.

IKE uses the specified PKI domains for enrollment, authentication, certificate issuing, validation, and signature. If you do not specify any PKI domains, IKE uses all PKI domains configured on the device.

Follow these restrictions and guidelines for the device to obtain the CA certificate during IKE negotiation:

- On the initiator:
  - If the IKE profile has a PKI domain and the automatic certificate request mode is configured for the PKI domain, the initiator automatically obtains the CA certificate.
  - If the IKE profile has no PKI domain, you must manually obtain the CA certificate.
- On the responder:
  - If main mode is used in IKE phase 1, the responder does not automatically obtain the CA certificate. You must manually obtain the CA certificate.
  - If aggressive mode is used in IKE phase 1, the responder automatically obtains the CA certificate if the following conditions are met:
    - A matching IKE profile is found.
    - An PKI domain is specified in the IKE profile.
    - The automatic certificate request mode is configured for the PKI domain.

    If the conditions are not met, you must manually obtain the CA certificate.

IKE first automatically obtains the CA certificate, and then requests a local certificate. If the CA certificate already exists locally, IKE automatically requests a local certificate.

Examples

Specify PKI domain **abc** for IKE profile 1.

```
<Sysname> system-view
[Sysname] ike profile 1
[Sysname-ike-profile-1] certificate domain abc
```

Related commands

authentication-method

pki domain

description

Use **description** to configure a description for an IKE proposal.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

An IKE proposal does not have a description.

Views

IKE proposal view

Predefined user roles

network-admin

Parameters

text: Specifies the description, a case-sensitive string of 1 to 80 characters.

Usage guidelines

When multiple IKE proposals exist, you configure different descriptions for them to distinguish them.

Examples

Configure a description of **test** for IKE proposal 1.

```
<Sysname> system-view
[Sysname] ike proposal 1
[Sysname-ike-proposal-1] description test
```

dh

Use **dh** to specify the DH group to be used for key negotiation in IKE phase 1.

Use **undo dh** to restore the default.

Syntax

In non-FIPS mode:

dh { **group1** | **group14** | **group19** | **group2** | **group20** | **group24** | **group5** }

undo dh

In FIPS mode:

dh { **group14** | **group19** | **group20** | **group24** }

undo dh

Default

In non-FIPS mode:

The 768-bit Diffie-Hellman group (**group1**) is used.

In FIPS mode:

The 2048-bit Diffie-Hellman group (**group14**) is used.

Views

IKE proposal view

Predefined user roles

network-admin

Parameters

group1: Uses the 768-bit Diffie-Hellman group.

group14: Uses the 2048-bit Diffie-Hellman group.

group19: Uses the 256-bit Diffie-Hellman group.

group2: Uses the 1024-bit Diffie-Hellman group.

group20: Uses the 384-bit Diffie-Hellman group.

group24: Uses the 2048-bit Diffie-Hellman group with the 256-bit prime order subgroup.

group5: Uses the 1536-bit Diffie-Hellman group.

Usage guidelines

A DH group with a higher group number provides higher security but needs more time for processing. To achieve the best trade-off between processing performance and security, choose a proper Diffie-Hellman group for your network.

Examples

Specify the 2048-bit Diffie-Hellman group **group1** to be used for key negotiation in IKE phase 1 in IKE proposal 1.

```
<Sysname> system-view
[Sysname] ike proposal 1
[Sysname-ike-proposal-1] dh group14
```

Related commands

display ike proposal

display ike proposal

Use **display ike proposal** to display configuration information about all IKE proposals.

Syntax

display ike proposal

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

This command displays the configuration information about all IKE proposals in descending order of proposal priorities. If no IKE proposal is configured, this command displays the default IKE proposal.

Examples

Display the configuration information about all IKE proposals.

```
<Sysname> display ike proposal
 Priority Authentication Authentication Encryption  Diffie-Hellman Duration
             method       algorithm    algorithm       group      (seconds)
------------------------------------------------------------------------------
 1        RSA-SIG            SHA1        DES-CBC     Group 1        5000
 11       PRE-SHARED-KEY     SHA1        DES-CBC     Group 1        50000
 default  PRE-SHARED-KEY     SHA1       DES-CBC     Group 1        86400
```

Table 10 Command output

Field	Description
Priority	Priority of the IKE proposal
Authentication method	Authentication method used by the IKE proposal.
Authentication algorithm	Authentication algorithm used in the IKE proposal: • **MD5**—HMAC-MD5 algorithm. • **SHA1**—HMAC-SHA1 algorithm. • **SHA256**—HMAC-SHA256 algorithm. • **SHA384**—HMAC-SHA384 algorithm. • **SHA512**—HMAC-SHA512 algorithm.
Encryption algorithm	Encryption algorithm used by the IKE proposal: • **3DES-CBC**—168-bit 3DES algorithm in CBC mode. • **AES-CBC-128**—128-bit AES algorithm in CBC mode. • **AES-CBC-192**—192-bit AES algorithm in CBC mode. • **AES-CBC-256**—256-bit AES algorithm in CBC mode. • **DES-CBC**—56-bit DES algorithm in CBC mode.
Diffie-Hellman group	DH group used in IKE negotiation phase 1.
Duration (seconds)	IKE SA lifetime (in seconds) of the IKE proposal

Related commands

ike proposal

display ike sa

Use **display ike sa** to display information about IKE SAs.

Syntax

display ike sa [**verbose** [**connection-id** *connection-id* | **remote-address** [**ipv6**] *remote-address*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

verbose: Displays detailed information.

connection-id *connection-id*: Displays detailed information about IKE SAs by connection ID in the range of 1 to 2000000000.

remote-address: Displays detailed information about IKE SAs with the specified remote address.

ipv6: Specifies an IPv6 address.

remote-address: Remote IP address.

Usage guidelines

If you do not specify any parameters, this command displays summary information about all IKE SAs.

Examples

Display summary information about all IKE SAs.

```
<Sysname> display ike sa
    Connection-ID  Remote          Flag        DOI
  -----------------------------------------------------------
      1            202.38.0.2      RD          IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
```

Table 11 Command output

Field	Description
Connection-ID	Identifier of the IKE SA.
Remote	Remote IP address of the SA.
Flags	Status of the SA: • **RD--READY**—The SA has been established. • **RL--REPLACED**—The SA has been replaced by a new one and will be deleted later. • **FD-FADING**—The SA is in use, but it is about to expire and will be deleted soon. • **RK-REKEY**—The SA is a Rekey SA. • **Unknown**—The SA status is unknown.
DOI	Interpretation domain to which the SA belongs. **IPsec**—The SA belongs to an IPsec DOI.

Display detailed information about all IKE SAs.

```
<Sysname> display ike sa verbose
    -----------------------------------------------
    Connection ID: 2
    Outside VPN:
    Inside VPN:
    Profile: prof1
    Transmitting entity: Initiator
    -----------------------------------------------
    Local IP: 4.4.4.4
    Local ID type: IPV4_ADDR
    Local ID: 4.4.4.4

    Remote IP: 4.4.4.5
```

```
    Remote ID type: IPV4_ADDR
    Remote ID: 4.4.4.5

    Authentication-method: PRE-SHARED-KEY
    Authentication-algorithm: SHA1
    Encryption-algorithm: AES-CBC-128

    Life duration(sec): 86400
    Remaining key duration(sec): 86379
    Exchange-mode: Main
    Diffie-Hellman group: Group 1
    NAT traversal: Not detected

    Extend authentication: Enabled
    Assigned IP address: 192.168.2.1
```

Display detailed information about the IKE SA with a remote address of 4.4.4.5.

```
<Sysname> display ike sa verbose remote-address 4.4.4.5
    -------------------------------------------
    Connection ID: 2
    Outside VPN:
    Inside VPN:
    Profile: prof1
    Transmitting entity: Initiator
    -------------------------------------------
    Local IP: 4.4.4.4
    Local ID type: IPV4_ADDR
    Local ID: 4.4.4.4

    Remote IP: 4.4.4.5
    Remote ID type: IPV4_ADDR
    Remote ID: 4.4.4.5

    Authentication-method: PRE-SHARED-KEY
    Authentication-algorithm: SHA1
    Encryption-algorithm: AES-CBC-128

    Life duration(sec): 86400
    Remaining key duration(sec): 86379
    Exchange-mode: Main
    Diffie-Hellman group: Group 1
    NAT traversal: Not detected

    Extend authentication: Enabled
    Assigned IP address: 192.168.2.1
```

Table 12 Command output

Field	Description
Connection ID	Identifier of the IKE SA.

Field	Description
Outside VPN	This field is not supported in the current software version. MPLS L3VPN instance to which the receiving interface belongs.
Inside VPN	This field is not supported in the current software version. MPLS L3VPN instance to which the protected data belongs.
Profile	Name of the matching IKE profile found in the IKE SA negotiation. If no matching profile is found, this field displays nothing.
Transmitting entity	Role of the IKE negotiation entity: **Initiator** or **Responder**.
Local IP	IP address of the local gateway.
Local ID type	Identifier type of the local gateway.
Local ID	Identifier of the local gateway.
Remote IP	IP address of the remote gateway.
Remote ID type	Identifier type of the remote gateway.
Remote ID	Identifier of the remote security gateway.
Authentication-method	Authentication method used by the IKE proposal.
Authentication-algorithm	Authentication algorithm used by the IKE proposal: • **MD5**—HMAC-MD5 algorithm. • **SHA1**—HMAC-SHA1 algorithm. • **SHA256**—HMAC-SHA256 algorithm. • **SHA384**—HMAC-SHA384 algorithm. • **SHA512**—HMAC-SHA512 algorithm.
Encryption-algorithm	Encryption algorithm used by the IKE proposal: • **3DES-CBC**—168-bit 3DES algorithm in CBC mode. • **AES-CBC-128**—128-bit AES algorithm in CBC mode. • **AES-CBC-192**—192-bit AES algorithm in CBC mode. • **AES-CBC-256**—256-bit AES algorithm in CBC mode. • **DES-CBC**—56-bit DES algorithm in CBC mode.
Life duration(sec)	Lifetime of the IKE SA in seconds.
Remaining key duration(sec)	Remaining lifetime of the IKE SA in seconds.
Exchange-mode	IKE negotiation mode in phase 1: **Main** or **Aggressive**.
Diffie-Hellman group	DH group used for key negotiation in IKE phase 1.
NAT traversal	Whether a NAT gateway is detected.
Extend authentication	Whether extended authentication for clients is enabled.
Assigned IP address	IP address assigned to the remote peer. This field is not displayed if no IP address is assigned.

display ike statistics

Use **display ike statistics** to display IKE statistics.

Syntax

display ike statistics

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display IKE statistics.

```
<Sysname> display ike statistics
IKE statistics:
  No matching proposal: 0
  Invalid ID information: 0
  Unavailable certificate: 0
  Unsupported DOI: 0
  Unsupported situation: 0
  Invalid proposal syntax: 0
  Invalid SPI: 0
  Invalid protocol ID: 0
  Invalid certificate: 0
  Authentication failure: 0
  Invalid flags: 0
  Invalid message id: 0
  Invalid cookie: 0
  Invalid transform ID: 0
  Malformed payload: 0
  Invalid key information: 0
  Invalid hash information: 0
  Unsupported attribute: 0
  Unsupported certificate type: 0
  Invalid certificate authority: 0
  Invalid signature: 0
  Unsupported exchange type: 0
  No available SA: 1
  Retransmit timeout: 0
  Not enough memory: 0
  Enqueue fails: 0
```

Related commands

reset ike statistics

dpd

Use **dpd** to configure IKE DPD.

Use **undo dpd** to disable IKE DPD.

Syntax

dpd interval *interval* [**retry** *seconds*] { **on-demand** | **periodic** }

undo dpd interval

Default

IKE DPD is disabled.

Views

IKE profile view

Predefined user roles

network-admin

Parameters

interval *interval*: Specifies a DPD triggering interval in the range of 1 to 300 seconds.

retry *seconds*: Specifies the DPD retry interval in the range of 1 to 60 seconds. The default is 5 seconds.

on-demand: Triggers DPD on demand. The device triggers DPD if it has IPsec traffic to send and has not received any IPsec packets from the peer for the specified interval.

periodic: Triggers DPD at regular intervals. The device triggers DPD at the specified interval.

Usage guidelines

DPD is triggered periodically or on-demand. As a best practice, use the on-demand mode when the device communicates with a large number of IKE peers. For an earlier detection of dead peers, use the periodic triggering mode, which consumes more bandwidth and CPU.

When DPD settings are configured in both IKE profile view and system view, the DPD settings in IKE profile view apply. If DPD is not configured in IKE profile view, the DPD settings in system view apply.

It is a good practice to set the triggering interval longer than the retry interval so that a DPD detection does not occur during a DPD retry.

Examples

Configure DPD to be triggered every 10 seconds and every 5 seconds between retries if the peer does not respond.

```
<Sysname> system-view
[Sysname] ike profile 1
[Sysname-ike-profile-1] dpd interval 10 retry 5 on-demand
```

Related commands

ike dpd

encryption-algorithm

Use **encryption-algorithm** to specify an encryption algorithm for an IKE proposal.

Use **undo encryption-algorithm** to restore the default.

Syntax

In non-FIPS mode:

encryption-algorithm { **3des-cbc** | **aes-cbc-128** | **aes-cbc-192** | **aes-cbc-256** | **des-cbc** }

undo encryption-algorithm

In FIPS mode:

encryption-algorithm { **aes-cbc-128** | **aes-cbc-192** | **aes-cbc-256** }

undo encryption-algorithm

Default

In non-FIPS mode:

An IKE proposal uses the 56-bit DES encryption algorithm in CBC mode.

In FIPS mode:

An IKE proposal uses the 128-bit AES encryption algorithm in CBC mode.

Views

IKE proposal view

Predefined user roles

network-admin

Parameters

3des-cbc: Specifies the 3DES algorithm in CBC mode. The 3DES algorithm uses a 168-bit key for encryption.

aes-cbc-128: Specifies the AES algorithm in CBC mode. The AES algorithm uses a 128-bit key for encryption.

aes-cbc-192: Specifies the AES algorithm in CBC mode. The AES algorithm uses a 192-bit key for encryption.

aes-cbc-256: Specifies the AES algorithm in CBC mode. The AES algorithm uses a 256-bit key for encryption.

des-cbc: Specifies the DES algorithm in CBC mode. The DES algorithm uses a 56-bit key for encryption.

Examples

Use the 128-bit AES algorithm in CBC mode as the encryption algorithm for IKE proposal 1.

```
<Sysname> system-view
[Sysname] ike proposal 1
[Sysname-ike-proposal-1] encryption-algorithm aes-cbc-128
```

Related commands

display ike proposal

exchange-mode

Use **exchange-mode** to select an IKE negotiation mode for phase 1.

Use **undo exchange-mode** to restore the default.

Syntax

In non-FIPS mode:

exchange-mode { **aggressive** | **main** }

undo exchange-mode

In FIPS mode:

exchange-mode main

undo exchange-mode

Default

Main mode is used for phase 1.

Views

IKE profile view

Predefined user roles

network-admin

Parameters

aggressive: Specifies the aggressive mode.

main: Specifies the main mode.

Usage guidelines

As a best practice, specify the **aggressive** mode at the local end if the following conditions are met:

- The local end, for example, a dialup user, obtains an IP address automatically.
- Preshared key authentication is used.

Examples

Specify that IKE negotiation operates in main mode.

```
<Sysname> system-view
[Sysname] ike profile 1
[Sysname-ike-profile-1] exchange-mode main
```

Related commands

display ike proposal

ike dpd

Use **ike dpd** to configure global IKE DPD.

Use **undo ike dpd** to disable global IKE DPD.

Syntax

ike dpd interval *interval* [**retry** *seconds*] { **on-demand** | **periodic** }

undo ike dpd interval

Default

Global IKE DPD is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

interval *interval*: Specifies a DPD triggering interval in the range of 1 to 300 seconds.

retry *seconds*: Specifies the DPD retry interval in the range of 1 to 60 seconds. The default is 5 seconds.

on-demand: Triggers DPD on demand. The device triggers DPD if it has IPsec traffic to send and has not received any IPsec packets from the peer for the specified interval.

periodic: Triggers DPD at regular intervals. The device triggers DPD at the specified interval.

Usage guidelines

DPD is triggered periodically or on-demand. As a best practice, use the on-demand mode when the device communicates with a large number of IKE peers. For an earlier detection of dead peers, use the periodical triggering mode, which consumes more bandwidth and CPU.

When DPD settings are configured in both IKE profile view and system view, the DPD settings in IKE profile view apply. If DPD is not configured in IKE profile view, the DPD settings in system view apply.

It is a good practice to set the triggering interval longer than the retry interval so that a DPD detection does not occur during a DPD retry.

Examples

Configure DPD to be triggered every 10 seconds and every 5 seconds between retries if the peer does not respond.

```
<Sysname> system-view
[Sysname] ike dpd interval 10 retry 5 on-demand
```

Related commands

dpd

ike identity

Use **ike identity** to specify the global identity used by the local end during IKE negotiations.

Use **undo ike identity** to restore the default.

Syntax

ike identity { **address** { *ipv4-address* | **ipv6** *ipv6-address* }| **dn** | **fqdn** [*fqdn-name*] | **user-fqdn** [*user-fqdn-name*] }

undo ike identity

Default

The IP address of the interface where the IPsec policy applies is used as the IKE identity.

Views

System view

Predefined user roles

network-admin

Parameters

address { *ipv4-address* | **ipv6** *ipv6-address* }: Uses an IPv4 or IPv6 address as the identity.

dn: Uses the DN in the digital signature as the identity.

fqdn *fqdn-name*: Uses the FQDN name as the identity. The *fqdn-name* argument is a case-sensitive string of 1 to 255 characters, for example, www.test.com. If you do not specify this argument, the device name configured by using the **sysname** command is used as the local FQDN.

user-fqdn *user-fqdn-name*: Uses the user FQDN name as the identity. The *user-fqdn-name* argument is a case-sensitive string of 1 to 255 characters, for example, abc@test.com. If you do not specify this argument, the device name configured by using the **sysname** command is used as the user FQDN.

Usage guidelines

The global local identity can be used for all IKE SA negotiations. The local identity (set by the **local-identity** command for an IKE profile) can be used only for IKE SA negotiations that use the IKE profile.

If the local authentication method is signature authentication, you can set an identity of any type. If the local authentication method is preshared key authentication, you cannot set the DN as the identity.

The **ike signature-identity from-certificate** command sets the local device to always use the identity information obtained from the local certificate for signature authentication. If the **ike signature-identity from-certificate** command is not set, the **local-identity** command configuration, if configured, takes precedence over the **ike identity** command configuration.

Examples

Specify IP address 2.2.2.2 as the identity.

```
<sysname> system-view
[sysname] ike identity address 2.2.2.2
```

Related commands

local-identity

ike signature-identity from-certificate

ike invalid-spi-recovery enable

Use **ike invalid-spi-recovery enable** to enable invalid security parameter index (SPI) recovery.

Use **undo ike invalid-spi-recovery enable** to disable invalid SPI recovery.

Syntax

ike invalid-spi-recovery enable

undo ike invalid-spi-recovery enable

Default

Invalid SPI recovery is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

IPsec "black hole" occurs when one IPsec peer fails (for example, a peer can fail if a reboot occurs). One peer fails and loses its SAs with the other peer. When an IPsec peer receives a data packet for which it cannot find an SA, an invalid SPI is encountered. The peer drops the data packet and tries to send an SPI invalid notification to the data originator. This notification is sent by using the IKE SA. When no IKE SA is available, the notification is not sent. The originating peer continues sending the data by using the IPsec SA that has the invalid SPI, and the receiving peer keeps dropping the traffic.

The invalid SPI recovery feature enables the receiving peer to set up an IKE SA with the originator so that an SPI invalid notification can be sent. Upon receiving the notification, the originating peer deletes the IPsec SA that has the invalid SPI. If the originator has data to send, new SAs will be set up.

Use caution when you enable the invalid SPI recovery feature, because using this feature can result in a DoS attack. Attackers can make a great number of invalid SPI notifications to the same peer.

Examples

Enable invalid SPI recovery.

```
<Sysname> system-view
[Sysname] ike invalid-spi-recovery enable
```

ike keepalive interval

Use **ike keepalive interval** to set the IKE keepalive interval.

Use **undo ike keepalive interval** to restore the default.

Syntax

ike keepalive interval *interval*

undo ike keepalive interval

Default

No IKE keepalives are sent.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the number of seconds between IKE keepalives, in the range of 20 to 28800.

Usage guidelines

To detect the status of the peer, configure IKE DPD instead of the IKE keepalive feature, unless IKE DPD is not supported on the peer.

The keepalive timeout time configured at the local must be longer than the keepalive interval configured at the peer. Because more than three consecutive packets are rarely lost on a network, you can set the keepalive timeout time to three times as long as the keepalive interval.

Examples

Set the keepalive interval to 200 seconds

```
<Sysname> system-view
[Sysname] ike keepalive interval 200
```

Related commands

ike keepalive timeout

ike keepalive timeout

Use **ike keepalive timeout** to set the IKE keepalive timeout time.

Use **undo ike keepalive timeout** to restore the default.

Syntax

ike keepalive timeout *seconds*

undo ike keepalive timeout

Default

The IKE keepalive timeout time is not set.

Views

System view

Predefined user roles

network-admin

Parameters

seconds: Specifies the number of seconds between IKE keepalives. The value range for this argument is 20 to 28800.

Usage guidelines

If the local end receives no keepalive packets from the peer during the timeout time, the IKE SA is deleted along with the IPsec SAs it negotiated.

The keepalive timeout time configured at the local end must be longer than the keepalive interval configured at the peer. Because more than three consecutive packets are rarely lost on a network, you can set the keepalive timeout time to three times as long as the keepalive interval.

Examples

Set the keepalive timeout time to 20 seconds.

```
<Sysname> system-view
[Sysname] ike keepalive timeout 20
```

Related commands

ike keepalive interval

ike keychain

Use **ike keychain** to create an IKE keychain and enter its view, or enter the view of an existing IKE keychain.

Use **undo ike keychain** to delete an IKE keychain.

Syntax

ike keychain *keychain-name*

undo ike keychain *keychain-name*

Default

No IKE keychains exist.

Views

System view

Predefined user roles

network-admin

Parameters

keychain-name: Specifies an IKE keychain name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

To use preshared key authentication, you must create and specify an IKE keychain for the IKE profile.

Examples

Create IKE keychain **key1** and enter its view.

```
<Sysname> system-view
[Sysname] ike keychain key1
[Sysname-ike-keychain-key1]
```

Related commands

authentication-method

pre-shared-key

ike limit

Use **ike limit** to set the maximum number of half-open or established IKE SAs.

Use **undo ike limit** to restore the default.

Syntax

ike limit { **max-negotiating-sa** *negotiation-limit* | **max-sa** *sa-limit* }

undo ike limit { **max-negotiating-sa** | **max-sa** }

Default

There is no limit to the maximum number of half-open or established IKE SAs.

Views

System view

Predefined user roles

network-admin

Parameters

max-negotiating-sa *negotiation-limit*: Specifies the maximum number of half-open IKE SAs and IPsec SAs. The value range for the *negotiation-limit* argument is 1 to 99999.

max-sa *sa-limit*: Specifies the maximum number of established IKE SAs. The value range for the *sa-limit* argument is 1 to 99999.

Usage guidelines

The supported maximum number of half-open IKE SAs depends on the device's processing capability. Adjust the maximum number of half-open IKE SAs to make full use of the device's processing capability without affecting the IKE SA negotiation efficiency.

The supported maximum number of established IKE SAs depends on the device's memory space. Adjust the maximum number of established IKE SAs to make full use of the device's memory space without affecting other applications in the system.

Examples

Set the maximum number of half-open IKE SAs and IPsec SAs to 200.

```
<Sysname> system-view
[Sysname] ike limit max-negotiating-sa 200
```

Set the maximum number of established IKE SAs to 5000.

```
<Sysname> system-view
[Sysname] ike limit max-sa 5000
```

ike nat-keepalive

Use **ike nat-keepalive** to set the NAT keepalive interval.

Use **undo ike nat-keepalive** to restore the default.

Syntax

ike nat-keepalive *seconds*

undo ike nat-keepalive

Default

The NAT keepalive interval is 20 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

seconds: Specifies the NAT keepalive interval in seconds, in the range of 5 to 300.

Usage guidelines

This command takes effect only for a device that resides in the private network behind a NAT gateway. The device behind the NAT gateway needs to send NAT keepalives to its peer to keep the NAT session alive, so that the peer can access the device.

The NAT keepalive interval must be shorter than the NAT session lifetime.

Examples

Set the NAT keepalive interval to 5 seconds.

```
<Sysname> system-view
[Sysname] ike nat-keepalive 5
```

ike profile

Use **ike profile** to create an IKE profile and enter its view, or enter the view of an existing IKE profile.

Use **undo ike profile** to delete an IKE profile.

Syntax

ike profile *profile-name*

undo ike profile *profile-name*

Default

No IKE profiles exist.

Views

System view

Predefined user roles

network-admin

Parameters

profile-name: Specifies an IKE profile name, a case-insensitive string of 1 to 63 characters.

Examples

Create IKE profile 1 and enter its view.

```
<Sysname> system-view
[Sysname] ike profile 1
[Sysname-ike-profile-1]
```

ike proposal

Use **ike proposal** to create an IKE proposal and enter its view, or enter the view of an existing IKE proposal.

Use **undo ike proposal** to delete an IKE proposal.

Syntax

ike proposal proposal-number

undo ike proposal *proposal-number*

Default

An IKE proposal exists, which has the lowest priority and uses the following settings:

- **Encryption algorithm**—DES-CBC in non-FIPS mode and AES-CBC-128 in FIPS mode.
- **Authentication algorithm**—HMAC-SHA1 in non-FIPS mode and SHA256 in FIPS mode.
- **Authentication method**—Preshared key authentication.
- **DH group**—768-bit Diffie-Hellman group in non-FIPS mode and 2048-bit Diffie-Hellman group in FIPS mode.
- **IKE SA lifetime**—86400 seconds.

You cannot change the settings of the default IKE proposal.

Views

System view

Predefined user roles

network-admin

Parameters

proposal-number: Specifies an IKE proposal number in the range of 1 to 65535. The lower the number, the higher the priority of the IKE proposal.

Usage guidelines

During IKE negotiation:

- The initiator sends its IKE proposals to the peer.
  - If the initiator is using an IPsec policy with an IKE profile, the initiator sends all IKE proposals specified for the IKE profile to the peer. An IKE proposal specified earlier for the IKE profile has a higher priority.
  - If the initiator is using an IPsec policy with no IKE profile, the initiator sends all its IKE proposals to the peer. An IKE proposal with a smaller number has a higher priority.
- The peer searches its own IKE proposals for a match. The search starts from the IKE proposal with the highest priority and proceeds in descending order of priority until a match is found. The matching IKE proposals are used to establish the IKE SA. If all user-defined IKE proposals are mismatched, the two peers use their default IKE proposals to establish the IKE SA.

Examples

Create IKE proposal 1 and enter its view.

```
<Sysname> system-view
[Sysname] ike proposal 1
[Sysname-ike-proposal-1]
```

Related commands

display ike proposal

ike signature-identity from-certificate

Use **ike signature-identity from-certificate** to configure the local device to obtain the identity information from the local certificate for signature authentication.

Use **undo ike signature-identity from-certificate** to restore the default.

Syntax

ike signature-identity from-certificate

undo ike signature-identity from-certificate

Default

The local end uses the identity information specified by the **local-identity** or **ike identity** command for signature authentication.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command requires the local device to always use the identity information in the local certificate for signature authentication, regardless of the **local-identity** or **ike identity** configuration.

Configure this command when the aggressive mode and signature authentication are used and the device interconnects with a Comware 5-based peer device. Comware 5 supports only DN for signature authentication.

If the **ike signature-identity from-certificate** command is not configured, the **local-identity** command configuration, if configured, takes precedence over the **ike identity** command configuration.

Examples

Configure the local device to always obtain the identity information from the local certificate for signature authentication.

```
<Sysname> system-view
[sysname] ike signature-identity from-certificate
```

Related commands

local-identity

ike identity

keychain

Use **keychain** to specify an IKE keychain for preshared key authentication.

Use **undo keychain** to remove an IKE keychain.

Syntax

keychain *keychain-name*

undo keychain *keychain-name*

Default

No IKE keychain is specified for preshared key authentication.

Views

IKE profile view

Predefined user roles

network-admin

Parameters

keychain-name: Specifies an IKE keychain name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can specify a maximum of six IKE keychains for an IKE profile. An IKE keychain specified earlier has a higher priority.

Examples

Specify IKE keychain **abc** for IKE profile **1**.

```
<Sysname> system-view
[Sysname] ike profile 1
[Sysname-ike-profile-1] keychain abc
```

Related commands

ike keychain

local-identity

Use **local-identity** to configure the local ID, the ID that the device uses to identify itself to the peer during IKE negotiation.

Use **undo local-identity** to restore the default.

Syntax

local-identity { **address** { *ipv4-address* | **ipv6** *ipv6-address* } | **dn** | **fqdn** [*fqdn-name*] | **user-fqdn** [*user-fqdn-name*] }

undo local-identity

Default

No local ID is configured for an IKE profile. An IKE profile uses the local ID configured in system view by using the **ike identity** command. If the local ID is not configured in system view, the IKE profile uses the IP address of the interface to which the IPsec policy is applied as the local ID.

Views

IKE profile view

Predefined user roles

network-admin

Parameters

address { *ipv4-address* | **ipv6** *ipv6-address* }: Uses an IPv4 or IPv6 address as the local ID.

dn: Uses the DN in the local certificate as the local ID.

fqdn *fqdn-name*: Uses an FQDN as the local ID. The *fqdn-name* argument is a case-sensitive string of 1 to 255 characters, such as www.test.com. If you do not specify this argument, the device name configured by using the **sysname** command is used as the local FQDN.

user-fqdn *user-fqdn-name*: Uses a user FQDN as the local ID. The *user-fqdn-name* argument is a case-sensitive string of 1 to 255 characters, such as adc@test.com. If you do not specify this argument, the device name configured by using the **sysname** command is used as the user FQDN.

Usage guidelines

For digital signature authentication, the device can use any type of ID. For preshared key authentication, the device can use any type of ID other than the DN.

In digital signature authentication, if the local ID is an IP address that is different from the IP address in the local certificate, the device uses its FQDN instead. The FQDN is the device name configured by using the **sysname** command.

The initiator uses the local ID to identify itself to the responder. The responder compares the initiator's ID with the peer IDs configured by the **match remote** command to look for a matching IKE profile.

An IKE profile can have only one local ID.

An IKE profile with no local ID specified uses the local ID configured by using the **ike identity** command in system view.

Examples

Set the local ID to IP address **2.2.2.2**.

```
<Sysname> system-view
[Sysname] ike profile prof1
[Sysname-ike-profile-prof1] local-identity address 2.2.2.2
```

Related commands

match remote

ike identity

match local address (IKE keychain view)

Use **match local address** to specify a local interface or IP address to which an IKE keychain can be applied.

Use **undo match local address** to restore the default.

Syntax

match local address { *interface-type interface-number* | { *ipv4-address* | **ipv6** *ipv6-address* } }

undo match local address

Default

An IKE keychain can be applied to any local interface or IP address.

Views

IKE keychain view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies a local interface. It can be any Layer 3 interface.

ipv4-address: Specifies the IPv4 address of a local interface.

ipv6 *ipv6-address*: Specifies the IPv6 address of a local interface.

Usage guidelines

Use this command to specify which address or interface can use the IKE keychain for IKE negotiation. Specify the local address configured in IPsec policy or IPsec policy template view (using the **local-address** command) for this command. If no local address is configured, specify the IP address of the interface that uses the IPsec policy.

You can specify a maximum of six IKE keychains for an IKE profile. An IKE keychain specified earlier has a higher priority. To give an IKE keychain a higher priority, you can configure this command for the keychain. For example, suppose you specified IKE keychain A before specifying IKE keychain B, and you configured the peer ID 2.2.0.0/16 for IKE keychain A and the peer ID 2.2.2.0/24 for IKE keychain B. For the local interface with the IP address 3.3.3.3 to negotiate with the peer 2.2.2.6, IKE keychain A is preferred because IKE keychain A was specified earlier. To use IKE keychain B, you can use this command to restrict the application scope of IKE keychain B to address 3.3.3.3.

Examples

Create IKE keychain **key1**.

```
<Sysname> system-view
[Sysname] ike keychain key1
```

Apply IKE keychain **key1** to IP address 2.2.2.2.

```
[sysname-ike-keychain-key1] match local address 2.2.2.1
```

match local address (IKE profile view)

Use **match local address** to specify a local interface or IP address to which an IKE profile can be applied.

Use **undo match local address** to restore the default.

Syntax

match local address { *interface-type interface-number* | { *ipv4-address* | **ipv6** *ipv6-address* } }

undo match local address

Default

An IKE profile can be applied to any local interface or IP address.

Views

IKE profile view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies a local interface. It can be any Layer 3 interface.

ipv4-address: Specifies the IPv4 address of a local interface.

ipv6 *ipv6-address*: Specifies the IPv6 address of a local interface.

Usage guidelines

Use this command to specify which address or interface can use the IKE profile for IKE negotiation. Specify the local address configured in IPsec policy or IPsec policy template view (using the **local-address** command) for this command. If no local address is configured, specify the IP address of the interface that uses the IPsec policy.

An IKE profile configured earlier has a higher priority. To give an IKE profile that is configured later a higher priority, you can configure this command for the profile. For example, suppose you configured IKE profile A before configuring IKE profile B, and you configured the **match remote identity address range 2.2.2.1 2.2.2.100** command for IKE profile A and the **match remote identity address range 2.2.2.1 2.2.2.10** command for IKE profile B. For the local interface with the IP address 3.3.3.3 to negotiate with the peer 2.2.2.6, IKE profile A is preferred because IKE profile A was configured earlier. To use IKE profile B, you can use this command to restrict the application scope of IKE profile B to address 3.3.3.3.

Examples

Create IKE profile **prof1**.

```
<Sysname> system-view
[Sysname] ike profile prof1
```

Apply IKE profile **prof1** to IP address 2.2.2.2.

```
[sysname-ike-profile-prof1] match local address 2.2.2.1
```

match remote

Use **match remote** to configure a peer ID for IKE profile matching.

Use **undo match remote** to delete a peer ID for IKE profile matching.

Syntax

match remote { **certificate** *policy-name* | **identity** { **address** { { *ipv4-address* [*mask* | *mask-length*] | **range** *low-ipv4-address high-ipv4-address* } | **ipv6** { *ipv6-address* [*prefix-length*] | **range** *low-ipv6-address high-ipv6-address* } } | **fqdn** *fqdn-name* | **user-fqdn** *user-fqdn-name* } }

undo match remote { **certificate** *policy-name* | **identity** { **address** { { *ipv4-address* [*mask* | *mask-length*] | **range** *low-ipv4-address high-ipv4-address* } | **ipv6** { *ipv6-address* [*prefix-length*] | **range** *low-ipv6-address high-ipv6-address* } } | **fqdn** *fqdn-name* | **user-fqdn** *user-fqdn-name* } }

Default

No peer ID is configured for IKE profile matching.

Views

IKE profile view

Predefined user roles

network-admin

Parameters

certificate *policy-name*: Uses the DN in the peer's digital certificate as the peer ID for IKE profile matching. The *policy-name* argument is a string of 1 to 31 characters.

identity: Uses the specified information as the peer ID for IKE profile matching. The specified information is configured on the peer by using the **local-identity** command.

- **address** *ipv4-address* [*mask* | *mask-length*]: Uses an IPv4 host address or an IPv4 subnet address as the peer ID for IKE profile matching. The *mask-length* argument is in the range of 0 to 32. If you do not specify a mask or mask length, the 32-bit mask is used.
- **address range** *low-ipv4-address high-ipv4-address*: Uses a range of IPv4 addresses as the peer ID for IKE profile matching. The end address must be higher than the start address.
- **address ipv6** *ipv6-address* [*prefix-length*]: Uses an IPv6 host address or an IPv6 subnet address as the peer ID for IKE profile matching. The *prefix-length* argument is in the range of 0 to 128. If you do not specify a prefix length, the 128-bit prefix is used.
- **address ipv6 range** *low-ipv6-address high-ipv6-address*: Uses a range of IPv6 addresses as the peer ID for IKE profile matching. The end address must be higher than the start address.
- **fqdn** *fqdn-name*: Uses the peer's FQDN as the peer ID for IKE profile matching. The *fqdn-name* argument is a case-sensitive string of 1 to 255 characters, such as www.test.com.
- **user-fqdn** *user-fqdn-name*: Uses the peer's user FQDN as the peer ID for IKE profile matching. The *user-fqdn-name* argument is a case-sensitive string of 1 to 255 characters, such as adc@test.com.

Usage guidelines

When an end needs to select an IKE profile, it compares the peer's ID received with the peer IDs of its local IKE profiles. If a match is found, it uses the IKE profile with the matching peer ID for IKE negotiation.

Each IKE profile must have at least one peer ID configured. To make sure only one IKE profile is matched for a peer, do not configure the same peer ID for two or more IKE profiles. If you configure the same peer ID for two or more IKE profiles, which IKE profile is selected for IKE negotiation is unpredictable.

For an IKE profile, you can configure multiple peer IDs. A peer ID configured earlier has a higher priority.

Examples

Create IKE profile **prof1**.

```
<Sysname> system-view
[Sysname] ike profile prof1
```

Configure a peer ID with the identity type of FQDN and the value of **www.test.com**.

```
[Sysname-ike-profile-prof1] match remote identity fqdn www.test.com
```

Configure a peer ID with the identity type of IP address and the value of **10.1.1.1**.

```
[Sysname-ike-profile-prof1] match remote identity address 10.1.1.1
```

Related commands

local-identity

pre-shared-key

Use **pre-shared-key** to configure a preshared key.

Use **undo pre-shared-key** to delete a preshared key.

Syntax

In non-FIPS mode:

pre-shared-key { **address** { *ipv4-address* [*mask* | *mask-length*] | **ipv6** *ipv6-address* [*prefix-length*] } | **hostname** *host-name* } **key** { **cipher** | **simple** } *string*

undo pre-shared-key { **address** { *ipv4-address* [*mask* | *mask-length*] | **ipv6** *ipv6-address* [*prefix-length*] } | **hostname** *host-name* }

In FIPS mode:

pre-shared-key { **address** { *ipv4-address* [*mask* | *mask-length*] | **ipv6** *ipv6-address* [*prefix-length*] } | **hostname** *host-name* } **key** [**cipher** *string*]

undo pre-shared-key { **address** { *ipv4-address* [*mask* | *mask-length*] | **ipv6** *ipv6-address* [*prefix-length*] } | **hostname** *host-name* }

Default

No preshared key is configured.

Views

IKE keychain view

Predefined user roles

network-admin

Parameters

address: Specifies a peer by its address.

ipv4-address: Specifies the IPv4 address of the peer.

mask: Specifies the mask in dotted decimal notation. The default mask is 255.255.255.255.

mask-length: Specifies the mask length in the range of 0 to 32. The default mask length is 32.

ipv6: Specifies an IPv6 peer.

ipv6-address: Specifies the IPv6 address of the peer.

prefix-length: Specifies the prefix length in the range of 0 to 128. The default prefix length is 128.

hostname *host-name*: Specifies a peer by its hostname, a case-sensitive string of 1 to 255 characters.

key: Specifies a preshared key.

cipher: Specifies a preshared key in encrypted form.

simple: Specifies a preshared key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the preshared key. The key is case sensitive. In non-FIPS mode, its plaintext form is a string of 1 to 128 characters and its encrypted form is a string of 1 to 201 characters. In FIPS mode, its plaintext form is a string of 1 to 128 characters and its encrypted form is a string of 15 to 201 characters.

Usage guidelines

The address option or the hostname option specifies the peer with which the device can use the preshared key to perform IKE negotiation.

Two peers must be configured with the same preshared key to pass preshared key authentication.

In FIPS mode, if you do not specify the **cipher** *string* option, you specify a plaintext preshared key in interactive mode. The key is a case-sensitive string of 15 to 128 characters, and it must contain uppercase and lowercase letters, digits, and special characters other than the question mark (?). In non-FIPS mode, this command does not support configuring a preshared key in interactive mode.

Examples

Create IKE keychain **key1** and enter IKE keychain view.

```
<Sysname> system-view
[Sysname] ike keychain key1
```

Set the preshared key to be used for IKE negotiation with peer 1.1.1.2 to **123456TESTplat&!**.

```
[Sysname-ike-keychain-key1] pre-shared-key address 1.1.1.2 255.255.255.255 key simple
123456TESTplat&!
```

Related commands

authentication-method

keychain

priority (IKE keychain view)

Use **priority** to specify a priority for an IKE keychain.

Use **undo priority** to restore the default.

Syntax

priority *priority*

undo priority

Default

The priority of an IKE keychain is 100.

Views

IKE keychain view

Predefined user roles

network-admin

Parameters

priority *priority*: Specifies a priority number in the range of 1 to 65535. The lower the priority number, the higher the priority.

Usage guidelines

To determine the priority of an IKE keychain, the device examines the existence of the **match local address** command before examining the priority number. An IKE keychain with the **match local address** command configured has a higher priority than an IKE keychain that does not have the **match local address** command configured.

Examples

Set the priority to 10 for IKE keychain **key1**.

```
<Sysname> system-view
[Sysname] ike keychain key1
[Sysname-ike-keychain-key1] priority 10
```

priority (IKE profile view)

Use **priority** to specify a priority for an IKE profile.

Use **undo priority** to restore the default.

Syntax

priority *priority*

undo priority

Default

The priority of an IKE profile is 100.

Views

IKE profile view

Predefined user roles

network-admin

Parameters

priority *priority*: Specifies a priority number in the range of 1 to 65535. The smaller the priority number, the higher the priority.

Usage guidelines

To determine the priority of an IKE profile, the device examines the existence of the **match local address** command before examining the priority number. An IKE profile with the **match local address** command configured has a higher priority than an IKE profile that does not have the **match local address** command configured.

Examples

Set the priority to 10 for IKE profile **prof1**.

```
<Sysname> system-view
[Sysname] ike profile prof1
[Sysname-ike-profile-prof1] priority 10
```

proposal

Use **proposal** to specify IKE proposals for an IKE profile.

Use **undo proposal** to restore the default.

Syntax

proposal *proposal-number*&<1-6>

undo proposal

Default

No IKE proposals are specified for an IKE profile and the IKE proposals configured in system view are used for IKE negotiation.

Views

IKE profile view

Predefined user roles

network-admin

Parameters

proposal-number&<1-6>: Specifies a space-separated list of up to six IKE proposals by their numbers in the range of 1 to 65535. An IKE proposal specified earlier has a higher priority.

Usage guidelines

When acting as the initiator, the device sends the specified IKE proposals to its peer for IKE negotiation. When acting as the responder, the device uses the IKE proposals configured in system view to match the IKE proposals received from the initiator.

Examples

Specify IKE proposal **10** for IKE profile **prof1**.

```
<Sysname> system-view
[Sysname] ike profile prof1
[Sysname-ike-profile-prof1] proposal 10
```

Related commands

ike proposal

reset ike sa

Use **reset ike sa** to delete IKE SAs.

Syntax

reset ike sa [**connection-id** *connection-id*]

Views

User view

Predefined user roles

network-admin

Parameters

connection-id *connection-id*: Specifies the connection ID of the IKE SA to be cleared, in the range of 1 to 2000000000.

Usage guidelines

When you delete an IKE SA, the device automatically sends a notification to the peer.

Examples

Display the current IKE SAs.

```
<Sysname> display ike sa
    Connection-ID  Remote            Flag        DOI
  -------------------------------------------------------------
      1            202.38.0.2        RD          IPsec
      2            202.38.0.3        RD          IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
```

Delete the IKE SA with the connection ID **2**.

```
<Sysname> reset ike sa connection-id 2
```

Display the current IKE SAs.

```
<Sysname> display ike sa

    Connection-ID  Remote            Flag        DOI
  -------------------------------------------------------------
       1            202.38.0.2        RD          IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
```

reset ike statistics

Use **reset ike statistics** command to clear IKE MIB statistics.

Syntax

reset ike statistics

Views

User view

Predefined user roles

network-admin

Examples

Clears IKE MIB statistics.

```
<Sysname> reset ike statistics
```

Related commands

snmp-agent trap enable ike

sa duration

Use **sa duration** to set the IKE SA lifetime for an IKE proposal.

Use **undo sa duration** to restore the default.

Syntax

sa duration *seconds*

undo sa duration

Default

The IKE SA lifetime is 86400 seconds for an IKE proposal.

Views

IKE proposal view

Predefined user roles

network-admin

Parameters

seconds: Specifies the IKE SA lifetime in seconds, in the range of 60 to 604800.

Usage guidelines

Before an IKE SA expires, IKE negotiates a new SA. The new SA takes effect immediately after it is negotiated. The old IKE SA will be cleared when it expires.

If the communicating peers are configured with different IKE SA lifetime settings, the smaller setting takes effect.

Examples

Set the IKE SA lifetime to 600 seconds for IKE **proposal 1**.

```
<Sysname> system-view
[Sysname] ike proposal 1
[Sysname-ike-proposal-1] sa duration 600
```

Related commands

display ike proposal

snmp-agent trap enable ike

Use **snmp-agent trap enable ike** command to enable SNMP notifications for IKE.

Use **undo snmp-agent trap enable ike** to disable SNMP notifications for IKE.

Syntax

snmp-agent trap enable ike [**attr-not-support** | **auth-failure** | **cert-type-unsupport** | **cert-unavailable** | **decrypt-failure** | **encrypt-failure** | **global** | **invalid-cert-auth** | **invalid-cookie** | **invalid-id** | **invalid-proposal** | **invalid-protocol** | **invalid-sign** | **no-sa-failure** | **proposal-add** | **proposal–delete** | **tunnel-start** | **tunnel-stop** | **unsupport-exch-type**] *

undo snmp-agent trap enable ike [**attr-not-support** | **auth-failure** | **cert-type-unsupport** | **cert-unavailable** | **decrypt-failure** | **encrypt-failure** | **global** | **invalid-cert-auth** | **invalid-cookie** | **invalid-id** | **invalid-proposal** | **invalid-protocol** | **invalid-sign** | **no-sa-failure** | **proposal-add** | **proposal–delete** | **tunnel-start** | **tunnel-stop** | **unsupport-exch-type**] *

Default

All SNMP notifications for IKE are disabled.

Views

System view

Predefined user roles

network-admin

Parameters

attr-not-support: Specifies notifications about attribute-unsupported failures.

auth-failure: Specifies notifications about authentication failures.

cert-type-unsupport: Specifies notifications about certificate-type-unsupported failures.

cert-unavailable: Specifies notifications about certificate-unavailable failures.

decrypt-failure: Specifies notifications about decryption failures.

encrypt-failure: Specifies notifications about encryption failures.

global: Specifies notifications globally.

invalid-cert-auth: Specifies notifications about invalid-certificate-authentication failures.

invalid-cookie: Specifies notifications about invalid-cookie failures.

invalid-id: Specifies notifications about invalid-ID failures.

invalid-proposal: Specifies notifications about invalid-IKE-proposal failures.

invalid-protocol: Specifies notifications about invalid-protocol failures.

invalid-sign: Specifies notifications about invalid-signature failures.

no-sa-failure: Specifies notifications about SA-not-found failures.

proposal-add: Specifies notifications about events of adding IKE proposals.

proposal-delete: Specifies notifications about events of deleting IKE proposals.

tunnel-start: Specifies notifications about events of creating IKE tunnels.

tunnel-stop: Specifies notifications about events of deleting IKE tunnels.

unsupport-exch-type: Specifies notifications about negotiation-type-unsupported failures.

Usage guidelines

If you do not specify any keywords, this command enables or disables all SNMP notifications for IKE.

To generate and output SNMP notifications for a specific IKE failure type or event type, perform the following tasks:

1. Enable SNMP notifications for IKE globally.
2. Enable SNMP notifications for the failure type or event type.

Examples

Enable SNMP notifications for IKE globally.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable ike global
```

Enable SNMP notifications for events of creating IKE tunnels.

```
[Sysname] snmp-agent trap enable ike tunnel-start
```

IKEv2 commands

address

Use **address** to specify the IP address or IP address range of an IKEv2 peer.

Use **undo address** to restore the default.

Syntax

address { *ipv4-address* [*mask* | *mask-length*] | **ipv6** *ipv6-address* [*prefix-length*] }

undo address

Default

The IKEv2 peer's IP address or IP address range is not specified.

Views

IKEv2 peer view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies the IPv4 address of the IKEv2 peer.

mask: Specifies the subnet mask of the IPv4 address.

mask-length: Specifies the subnet mask length of the IPv4 address, in the range of 0 to 32.

ipv6 *ipv6-address*: Specifies the IPv6 address of the IKEv2 peer.

prefix-length: Specifies the prefix length of the IPv6 address, in the range of 0 to 128.

Usage guidelines

Both the initiator and the responder can look up an IKEv2 peer by IP address in IKEv2 negotiation.

The IP addresses of different IKEv2 peers in the same IKEv2 keychain cannot be the same.

Examples

Create an IKEv2 keychain named **key1**.

```
<Sysname> system-view
[Sysname] ikev2 keychain key1
```

Create an IKEv2 peer named **peer1**.

```
[Sysname-ikev2-keychain-key1] peer peer1
```

Specify the IKEv2 peer's IP address 3.3.3.3 with subnet mask 255.255.255.0.

```
[Sysname-ikev2-keychain-key1-peer-peer1] address 3.3.3.3 255.255.255.0
```

Related commands

ikev2 keychain

peer

authentication-method

Use **authentication-method** to specify the local or remote identity authentication method.

Use **undo authentication-method** to remove the local or remote identity authentication method.

Syntax

authentication-method { **local** | **remote** } { **dsa-signature** | **ecdsa-signature** | **pre-share** | **rsa-signature** }

undo authentication-method local

undo authentication-method remote { **dsa-signature** | **ecdsa-signature** | **pre-share** | **rsa-signature** }

Default

No local or remote identity authentication method is specified.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

local: Specifies the local identity authentication method.

remote: Specifies the remote identity authentication method.

dsa-signature: Specifies the DSA signatures as the identity authentication method.

ecdsa-signature: Specifies the ECDSA signatures as the identity authentication method.

pre-share: Specifies the preshared key as the identity authentication method.

rsa-signature: Specifies the RSA signatures as the identity authentication method.

Usage guidelines

The local and remote identity authentication methods must both be specified and they can be different.

You can specify only one local identity authentication method. You can specify multiple remote identity authentication methods by executing this command multiple times when there are multiple remote ends whose authentication methods are unknown.

If you use RSA, DSA, or ECDSA signature authentication, you must specify PKI domains for obtaining certificates. You can specify PKI domains by using the **certificate domain** command in IKEv2 profile view. If you do not specify PKI domains in IKEv2 profile view, the PKI domains configured by the **pki domain** command in system view will be used.

If you specify the preshared key method, you must specify a preshared key for the IKEv2 peer in the keychain used by the IKEv2 profile.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

Specify the preshared key and RSA signatures as the local and remote authentication methods, respectively.

```
[Sysname-ikev2-profile-profile1] authentication local pre-share
[Sysname-ikev2-profile-profile1] authentication remote rsa-signature
```

Specify PKI domain **genl** as the PKI domain for obtaining certificates.

```
[Sysname-ikev2-profile-profile1] certificate domain genl
```

Specify IKEv2 keychain **keychain1**.

```
[Sysname-ikev2-profile-profile1] keychain keychain1
```

Related commands

display ikev2 profile

certificate domain (IKEv2 profile view)

keychain (IKEv2 profile view)

certificate domain

Use **certificate domain** to specify a PKI domain for signature authentication in IKEv2 negotiation.

Use **undo certificate domain** to remove a PKI domain for signature authentication in IKEv2 negotiation.

Syntax

certificate domain *domain-name* [**sign** | **verify**]

undo certificate domain *domain-name*

Default

PKI domains configured in system view are used for signature authentication.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters.

sign: Uses the local certificate in the PKI domain to generate a signature.

verify: Uses the CA certificate in the PKI domain to verify the remote end's certificate.

Usage guidelines

If you do not specify the **sign** or **verify** keyword, the PKI domain is used for both **sign** and **verify** purposes. You can specify a PKI domain for each purpose by executing this command multiple times. If you specify the same PKI domain for both purposes, the later configuration takes effect. For example, if you execute **certificate domain abc sign** and **certificate domain abc verify** successively, the PKI domain **abc** will be used only for verification.

If the local end uses RSA, DSA, or ECDSA signature authentication, you must specify a PKI domain for signature generation. If the remote end uses RSA, DSA, or ECDSA signature authentication, you must specify a PKI domain for verifying the remote end's certificate. If you do not specify PKI domains, the PKI domains configured in system view will be used.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
```

```
[Sysname] ikev2 profile profile1
```

Specify PKI domain **abc** for signature. Specify PKI domain **def** for verification.

```
[Sysname-ikev2-profile-profile1] certificate domain abc sign
[Sysname-ikev2-profile-profile1] certificate domain def verify
```

Related commands

authentication-method

pki domain

config-exchange

Use **config-exchange** to enable configuration exchange.

Use **undo config-exchange** to disable configuration exchange.

Syntax

config-exchange { **request** | **set** { **accept** | **send** } }

undo config-exchange { **request** | **set** { **accept** | **send** } }

Default

Configuration exchange is disabled.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

request: Enables the device to send request messages carrying the configuration request payload during the IKE_AUTH exchange.

set: Specifies the configuration set payload exchange.

accept: Enables the device to accept the configuration set payload carried in Info messages.

send: Enables the device to send Info messages carrying the configuration set payload.

Usage guidelines

The configuration exchange feature enables the local and remote ends to exchange configuration data, such as gateway address, internal IP address, and route. The exchange includes data request and response, and data push and response. The enterprise center can push IP addresses to branches. The branches can request IP addresses, but the requested IP addresses cannot be used.

You can specify both **request** and **set** for the device.

If you specify **request** for the local end, the remote end will respond if it can obtain the requested data.

If you specify **set send** for the local end, you must specify **set accept** for the remote end.

The device with **set send** specified pushes an IP address after the IKEv2 SA is set up if it does not receive any configuration request from the peer.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

Enable the local end to add the configuration request payload to the request message of IKE_AUTH exchange.

```
[Sysname-ikev2-profile-profile1] config-exchange request
```

Related commands

display ikev2 profile

dh

Use **dh** to specify DH groups to be used in IKEv2 key negotiation.

Use **undo group** to restore the default.

Syntax

In non-FIPS mode:

dh { **group1** | **group14** | **group2** | **group24** | **group5** | **group19** | **group20** } *

undo dh

In FIPS mode:

dh { **group14** | **group19** | **group20** } *

undo dh

Default

No DH group is specified for an IKEv2 proposal.

Views

IKEv2 proposal view

Predefined user roles

network-admin

Parameters

group1: Uses the 768-bit Diffie-Hellman group.

group2: Uses the 1024-bit Diffie-Hellman group.

group5: Uses the 1536-bit Diffie-Hellman group.

group14: Uses the 2048-bit Diffie-Hellman group.

group24: Uses the 2048-bit Diffie-Hellman group with the 256-bit prime order subgroup.

group19: Uses the 256-bit ECP Diffie-Hellman group.

group20: Uses the 384-bit ECP Diffie-Hellman group.

Usage guidelines

A DH group with a higher group number provides higher security but needs more time for processing. To achieve the best trade-off between processing performance and security, choose proper DH groups for your network.

You must specify a minimum of one DH group for an IKEv2 proposal. Otherwise, the proposal is incomplete and useless.

You can specify multiple DH groups for an IKEv2 proposal. A group specified earlier has a higher priority.

Examples

Specify DH group 1 for IKEv2 proposal 1.

```
<Sysname> system-view
[Sysname] ikev2 proposal 1
[Sysname-ikev2-proposal-1] dh group1
```

Related commands

ikev2 proposal

display ikev2 policy

Use **display ikev2 policy** to display the IKEv2 policy configuration.

Syntax

display ikev2 policy [*policy-name* | **default**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

policy-name: Specifies an IKEv2 policy by its name, a case-insensitive string of 1 to 63 characters.

default: Specifies the default IKEv2 policy.

Usage guidelines

If you do not specify any parameters, this command displays the configuration of all IKEv2 policies.

Examples

Display the configuration of all IKEv2 policies.

```
<Sysname> display ikev2 policy
IKEv2 policy: 1
  Priority: 100
  Match local address: 1.1.1.1
  Match local address ipv6: 1:1::1:1
  Match VRF:
  Proposal: 1
  Proposal: 2
IKEv2 policy: default
  Match VRF:
  Proposal: default
```

Table 13 Command output

Field	Description
IKEv2 policy	Name of the IKEv2 policy.
Priority	Priority of the IKEv2 policy.
Match local address	IPv4 address to which the IKEv2 policy can be applied.
Match local address ipv6	IPv6 address to which the IKEv2 policy can be applied.

Field	Description
Match VRF	This field is not supported in the current software version. VPN instance to which the IKEv2 policy can be applied.
Proposal	IKEv2 proposal that the IKEv2 policy uses.

Related commands

ikev2 policy

display ikev2 profile

Use **display ikev2 profile** to display the IKEv2 profile configuration.

Syntax

display ikev2 profile [*profile-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

profile-name: Specifies an IKEv2 profile by its name, a case-insensitive string of 1 to 63 characters. If you do not specify an IKEv2 profile, this command displays the configuration of all IKEv2 profiles.

Examples

Display the configuration of all IKEv2 profiles.

```
<Sysname> display ikev2 profile
IKEv2 profile: 1
  Priority: 100
  Match criteria:
    Local address 1.1.1.1
    Local address Vlan-interface100
    Local address 1:1::1:1
    Remote identity ipv4 address 3.3.3.3/32
    VRF vrf1
  Inside-vrf:
  Local identity: address 1.1.1.1
  Local authentication method: pre-share
  Remote authentication methods: pre-share
  Keychain: Keychain1
  Sign certificate domain:
     Domain1
     abc
  Verify certificate domain:
     Domain2
     yy
```

```
SA duration: 500
DPD: Interval 32, retry 23, periodic
Config-exchange: Request, Set send, Set accept
NAT keepalive: 10
AAA authorization: Domain domain1, username ikev2
```

Table 14 Command output

Field	Description
IKEv2 profile	Name of the IKEv2 profile.
Priority	Priority of the IKEv2 profile.
Match criteria	Criteria for looking up the IKEv2 profile.
Inside-vrf	This field is not supported in the current software version. Inside VRF instance.
Local identity	ID of the local end.
Local authentication method	Method that the local end uses for authentication.
Remote authentication methods	Methods that the remote end uses for authentication.
Keychain	IKEv2 keychain that the IKEv2 profile uses.
Sign certificate domain	PKI domain used for signature generation.
Verify certificate domain	PKI domain used for verifying the remote end's certificate.
SA duration	Lifetime of the IKEv2 SA.
DPD	DPD settings: • Detection interval in seconds. • Retry interval in seconds. • Detection mode, on demand or periodically. If DPD is disabled, this field displays **Disabled**.
Config-exchange	Configuration exchange settings: • **Request**—The local end sends request messages carrying the configuration request payload during the IKE_AUTH exchange. • **Set accept**—The local end accepts the configuration set payload carried in Info messages. • **Set send**—The local end sends Info messages carrying the configuration set payload.
NAT keepalive	NAT keepalive interval in seconds.
AAA authorization	This field is not supported in the current software version. AAA authorization settings: • ISP domain name. • Username.

Related commands

`ikev2 profile`

display ikev2 proposal

Use **`display ikev2 proposal`** to display the IKEv2 proposal configuration.

Syntax

display ikev2 proposal [*name* | **default**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name: Specifies an IKEv2 proposal by its name, a case-insensitive string of 1 to 63 characters.

default: Specifies the default IKEv2 proposal.

Usage guidelines

This command displays IKEv2 proposals in descending order of priorities. If you do not specify any parameters, this command displays the configuration of all IKEv2 proposals.

Examples

Display the configuration of all IKEv2 proposals.

```
<Sysname> display ikev2 proposal
IKEv2 proposal : 1
  Encryption: 3DES-CBC AES-CBC-128 AES-CTR-192 CAMELLIA-CBC-128
  Integrity: MD5 SHA256 AES-XCBC-MAC
  PRF: MD5 SHA256 AES-XCBC-MAC
  DH Group: MODP1024/Group2 MODP1536/Group5

IKEv2 proposal : default
  Encryption: AES-CBC-128 3DES-CBC
  Integrity: SHA1 MD5
  PRF: SHA1 MD5
  DH Group: MODP1536/Group5 MODP1024/Group2
```

Table 15 Command output

Field	Description
IKEv2 proposal	Name of the IKEv2 proposal.
Encryption	Encryption algorithms that the IKEv2 proposal uses.
Integrity	Integrity protection algorithms that the IKEv2 proposal uses.
PRF	PRF algorithms that the IKEv2 proposal uses.
DH Group	DH groups that the IKEv2 proposal uses.

Related commands

ikev2 proposal

display ikev2 sa

Use **display ikev2 sa** to display the IKEv2 SA information.

Syntax

display ikev2 sa [**count** | [{ **local** | **remote** } { *ipv4-address* | **ipv6** *ipv6-address* }] [**verbose** [**tunnel** *tunnel-id*]]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

count: Displays the number of IKEv2 SAs.

local: Displays IKEv2 SA information for a local IP address.

remote: Displays IKEv2 SA information for a remote IP address.

ipv4-address: Specifies a local or remote IPv4 address.

ipv6 *ipv6-address*: Specifies a local or remote IPv6 address.

verbose: Displays detailed information. If you do not specify this keyword, the command displays the summary information.

tunnel *tunnel-id*: Displays detailed IKEv2 SA information for an IPsec tunnel. The *tunnel-id* argument specifies an IPsec tunnel by its ID in the range of 1 to 2000000000.

Usage guidelines

If you do not specify any parameters, this command displays summary information about all IKEv2 SAs.

Examples

Display summary information about all IKEv2 SAs.

```
<Sysname> display ikev2 sa
     Tunnel ID          Local             Remote             Status
  ----------------------------------------------------------------------
     1                  1.1.1.1/500       1.1.1.2/500        EST
     2                  2.2.2.1/500       2.2.2.2/500        EST
  Status:
  IN-NEGO: Negotiating, EST: Established, DEL: Deleting
```

Display summary IKEv2 SA information for the remote IP address 1.1.1.2.

```
<Sysname> display ikev2 sa remote 1.1.1.2
     Tunnel ID          Local             Remote             Status
  ----------------------------------------------------------------------
     1                  1.1.1.1/500       1.1.1.2/500        EST
  Status:
  IN-NEGO: Negotiating, EST: Established, DEL: Deleting
```

Table 16 Command output

Field	Description
Tunnel ID	ID of the IPsec tunnel to which the IKEv2 SA belongs.
Local	Local IP address of the IKEv2 SA.
Remote	Remote IP address of the IKEv2 SA.

Field	Description
Status	Status of the IKEv2 SA: • **IN-NEGO (Negotiating)**—The IKEv2 SA is under negotiation. • **EST (Established)**—The IKEv2 SA has been set up. • **DEL (Deleting)**—The IKEv2 SA is about to be deleted.

Display detailed information about all IKEv2 SAs.

```
<Sysname> display ikev2 sa verbose
  Tunnel ID: 1
  Local IP/Port: 1.1.1.1/500
  Remote IP/Port: 1.1.1.2/500
  Outside VRF: -
  Inside VRF: -
  Local SPI: 8f8af3dbf5023a00
  Remote SPI: 0131565b9b3155fa

  Local ID type: FQDN
  Local ID: device_a
  Remote ID type: FQDN
  Remote ID: device_b

  Auth sign method: Pre-shared key
  Auth verify method: Pre-shared key
  Integrity algorithm: HMAC_MD5
  PRF algorithm: HMAC_MD5
  Encryption algorithm: AES-CBC-192

  Life duration: 86400 secs
  Remaining key duration: 85604 secs
  Diffie-Hellman group: MODP1024/Group2
  NAT traversal: Not detected
  DPD: Interval 20 secs, retry interval 2 secs
  Transmitting entity: Initiator

  Local window: 1
  Remote window: 1
  Local request message ID: 2
  Remote request message ID:2
  Local next message ID: 0
  Remote next message ID: 0

  Pushed IP address: 192.168.1.5
  Assigned IP address: 192.168.2.24
```

Display detailed IKEv2 SA information for the remote IP address 1.1.1.2.

```
<Sysname> display ikev2 sa remote 1.1.1.2 verbose
  Tunnel ID: 1
```

```
Local IP/Port: 1.1.1.1/500
Remote IP/Port: 1.1.1.2/500
Outside VRF: -
Inside VRF: -
Local SPI: 8f8af3dbf5023a00
Remote SPI: 0131565b9b3155fa

Local ID type: FQDN
Local ID: device_a
Remote ID type: FQDN
Remote ID: device_b

Auth sign method: Pre-shared key
Auth verify method: Pre-shared key
Integrity algorithm: HMAC_MD5
PRF algorithm: HMAC_MD5
Encryption algorithm: AES-CBC-192

Life duration: 86400 secs
Remaining key duration: 85604 secs
Diffie-Hellman group: MODP1024/Group2
NAT traversal: Not detected
DPD: Interval 30 secs, retry interval 10 secs
Transmitting entity: Initiator

Local window: 1
Remote window: 1
Local request message ID: 2
Remote request message ID: 2
Local next message ID: 0
Remote next message ID: 0

Pushed IP address: 192.168.1.5
Assigned IP address: 192.168.2.24
```

Table 17 Command output

Field	Description
Tunnel ID	ID of the IPsec tunnel to which the IKEv2 SA belongs.
Local IP/Port	IP address and port number of the local security gateway.
Remote IP/Port	IP address and port number of the remote security gateway.
Outside VRF	This field is not supported in the current software version. Name of the VPN instance to which the protected outbound data flow belongs. If the protected outbound data flow belongs to the public network, this field displays a hyphen (-).
Inside VRF	This field is not supported in the current software version. Name of the VPN instance to which the protected inbound data

Field	Description
	flow belongs. If the protected inbound data flow belongs to the public network, this field displays a hyphen (**-**).
Local SPI	SPI that the local end uses.
Remote SPI	SPI that the remote end uses.
Local ID type	ID type of the local security gateway.
Local ID	ID of the local security gateway.
Remote ID type	ID type of the remote security gateway.
Remote ID	ID of the remote security gateway.
Auth sign method	Signature method that the IKEv2 proposal uses in authentication.
Auth verify method	Verification method that the IKEv2 proposal uses in authentication.
Integrity algorithm	Integrity protection algorithms that the IKEv2 proposal uses.
PRF algorithm	PRF algorithms that the IKEv2 proposal uses.
Encryption algorithm	Encryption algorithms that the IKEv2 proposal uses.
Life duration	Lifetime of the IKEv2 SA, in seconds.
Remaining key duration	Remaining lifetime of the IKEv2 SA, in seconds.
Diffie-Hellman group	DH groups used in IKEv2 key negotiation.
NAT traversal	Whether a NAT gateway is detected between the local and remote ends.
DPD	DPD settings: • Detection interval in seconds. • Retry interval in seconds. If DPD is disabled, this field displays **Disabled**.
Transmitting entity	Role of the local end in IKEv2 negotiation, initiator or responder.
Local window	Window size that the local end uses.
Remote window	Window size that the remote end uses.
Local request message ID	ID of the request message that the local end is about to send.
Remote request message ID	ID of the request message that the remote end is about to send.
Local next message ID	ID of the message that the local end expects to receive.
Remote next message ID	ID of the message that the remote end expects to receive.
Pushed IP address	IP address pushed to the local end by the remote end.
Assigned IP address	IP address assigned to the remote end by the local end .

Display the number of IKEv2 SAs.

```
[Sysname] display ikev2 sa count
IKEv2 SAs count: 0
```

display ikev2 statistics

Use **display ikev2 statistics** to display IKEv2 statistics.

Syntax

display ikev2 statistics

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display IKEv2 statistics.

```
<Sysname> display ikev2 statistics
IKEv2 statistics:
  Unsupported critical payload: 0
  Invalid IKE SPI: 0
  Invalid major version: 0
  Invalid syntax: 0
  Invalid message ID: 0
  Invalid SPI: 0
  No proposal chosen: 0
  Invalid KE payload: 0
  Authentication failed: 0
  Single pair required: 0
  TS unacceptable: 0
  Invalid selectors: 0
  Temporary failure: 0
  No child SA: 0
  Unknown other notify: 0
  No enough resource: 0
  Enqueue error: 0
  No IKEv2 SA: 0
  Packet error: 0
  Other error: 0
  Retransmit timeout: 0
  DPD detect error: 0
  Del child for IPsec message: 1
  Del child for deleting IKEv2 SA: 1
  Del child for receiving delete message: 0
```

Related commands

reset ikev2 statistics

dpd

Use **dpd** to configure IKEv2 DPD.

Use **undo dpd** to disable IKEv2 DPD.

Syntax

dpd interval *interval* [**retry** *seconds*] { **on-demand** | **periodic** }

undo dpd interval

Default

IKEv2 DPD is disabled. The global IKEv2 DPD settings are used.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

interval *interval*: Specifies a DPD triggering interval in the range of 10 to 3600 seconds.

retry *seconds*: Specifies the DPD retry interval in the range of 2 to 60 seconds. The default is 5 seconds.

on-demand: Triggers DPD on demand. The device triggers DPD if it has IPsec traffic to send and has not received any IPsec packets from the peer for the specified interval.

periodic: Triggers DPD at regular intervals. The device triggers DPD at the specified interval.

Usage guidelines

DPD is triggered periodically or on-demand. As a best practice, use the on-demand mode when the device communicates with a large number of IKEv2 peers. For an earlier detection of dead peers, use the periodic triggering mode, which consumes more bandwidth and CPU.

The triggering interval must be longer than the retry interval, so that the device will not trigger a new round of DPD during a DPD retry.

Examples

Configure on-demand IKEv2 DPD. Set the DPD triggering interval to 10 seconds and the retry interval to 5 seconds.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
[Sysname-ikev2-profile-profile1] dpd interval 10 retry 5 on-demand
```

Related commands

ikev2 dpd

encryption

Use **encryption** to specify encryption algorithms for an IKEv2 proposal.

Use **undo encryption** to restore the default.

Syntax

In non-FIPS mode:

encryption { **3des-cbc** | **aes-cbc-128** | **aes-cbc-192** | **aes-cbc-256** | **aes-ctr-128** | **aes-ctr-192** | **aes-ctr-256** | **camellia-cbc-128** | **camellia-cbc-192** | **camellia-cbc-256** | **des-cbc** } *

undo encryption

In FIPS mode:

encryption { **aes-cbc-128** | **aes-cbc-192** | **aes-cbc-256** | **aes-ctr-128** | **aes-ctr-192** | **aes-ctr-256** } *

undo encryption

Default

No encryption algorithm is specified for an IKEv2 proposal.

Views

IKEv2 proposal view

Predefined user roles

network-admin

Parameters

3des-cbc: Specifies the 3DES algorithm in CBC mode, which uses a 168-bit key.

aes-cbc-128: Specifies the AES algorithm in CBC mode, which uses a 128-bit key.

aes-cbc-192: Specifies the AES algorithm in CBC mode, which uses a 192-bit key.

aes-cbc-256: Specifies the AES algorithm in CBC mode, which uses a 256-bit key.

aes-ctr-128: Specifies the AES algorithm in CTR mode, which uses a 128-bit key.

aes-ctr-192: Specifies the AES algorithm in CTR mode, which uses a 192-bit key.

aes-ctr-256: Specifies the AES algorithm in CTR mode, which uses a 256-bit key.

camellia-cbc-128: Specifies the Camellia algorithm in CBC mode, which uses a 128-bit key.

camellia-cbc-192: Specifies the Camellia algorithm in CBC mode, which uses a 192-bit key.

camellia-cbc-256: Specifies the Camellia algorithm in CBC mode, which uses a 256-bit key.

des-cbc: Specifies the DES algorithm in CBC mode, which uses a 56-bit key.

Usage guidelines

You must specify a minimum of one encryption algorithm for an IKEv2 proposal. Otherwise, the proposal is incomplete and useless. You can specify multiple encryption algorithms for an IKEv2 proposal. An algorithm specified earlier has a higher priority.

Examples

Specify the 168-bit 3DES algorithm in CBC mode as the encryption algorithm for IKE proposal **prop1**.

```
<Sysname> system-view
[Sysname] ikev2 proposal prop1
[Sysname-ikev2-proposal-prop1] encryption 3des-cbc
```

Related commands

ikev2 proposal

hostname

Use **hostname** to specify the host name of an IKEv2 peer.

Use **undo hostname** to restore the default.

Syntax

hostname *name*

undo hostname

Default

The IKEv2 peer's host name is not specified.

Views

IKEv2 peer view

Predefined user roles

network-admin

Parameters

name: Specifies the host name of the IKEv2 peer, a case-insensitive string of 1 to 253 characters.

Usage guidelines

Only the initiator can look up an IKEv2 peer by host name in IKEv2 negotiation, and the initiator must use an IPsec policy rather than an IPsec profile.

Examples

Create an IKEv2 keychain named **key1**.

```
<Sysname> system-view
[Sysname] ikev2 keychain key1
```

Create an IKEv2 peer named **peer1**.

```
[Sysname-ikev2-keychain-key1] peer peer1
```

Specify host name **test** of the IKEv2 peer.

```
[Sysname-ikev2-keychain-key1-peer-peer1] hostname test
```

Related commands

ikev2 keychain

peer

identity

Use **identity** to specify the ID of an IKEv2 peer.

Use **undo identity** to restore the default.

Syntax

identity { **address** { *ipv4-address* | **ipv6** { *ipv6-address* } } | **fqdn** *fqdn-name* | **email** *email-string* | **key-id** *key-id-string* }

undo identity

Default

The IKEv2 peer's ID is not specified.

Views

IKEv2 peer view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies the IPv4 address of the peer.

ipv6 *ipv6-address*: Specifies the IPv6 address of the peer.

fqdn *fqdn-name*: Specifies the FQDN of the peer. The *fqdn-name* argument is a case-sensitive string of 1 to 255 characters, such as www.test.com.

email *email-string*: Specifies the email address of the peer. The *email-string* argument is a case-sensitive string of 1 to 255 characters in the format defined by RFC 822, such as esec@test.com.

key-id *key-id-string*: Specifies the remote gateway's key ID. The *key-id-string* argument is a case-sensitive string of 1 to 255 characters, and is usually a vendor-specific string for doing proprietary types of identification.

Usage guidelines

Only the responder can look up an IKEv2 peer by ID in IKEv2 negotiation. The initiator does not know the peer ID when initiating the IKEv2 negotiation, so it cannot use an ID for IKEv2 peer lookup.

Examples

Create an IKEv2 keychain named **key1**.

```
<Sysname> system-view
[Sysname] ikev2 keychain key1
```

Create an IKEv2 peer named **peer1**.

```
[Sysname-ikev2-keychain-key1] peer peer1
```

Specify IPv4 address 1.1.1.2 as the ID of the IKEv2 peer.

```
[Sysname-ikev2-keychain-key1-peer-peer1] identity address 1.1.1.2
```

Related commands

ikev2 keychain

peer

identity local

Use **identity local** to configure the local ID, the ID that the device uses to identify itself to the peer during IKEv2 negotiation..

Use **undo identity local** to restore the default.

Syntax

identity local { **address** { *ipv4-address* | **ipv6** *ipv6-address* } | **dn** | **email** *email-string* | **fqdn** *fqdn-name* | **key-id** *key-id-string* }

undo identity local

Default

No local ID is configured. The IP address of the interface to which the IPsec policy is applied is used as the local ID.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

address { *ipv4-address* | **ipv6** *ipv6-address* }: Uses an IPv4 or IPv6 address as the local ID.

dn: Uses the DN in the local certificate as the local ID.

email *email-string*: Uses an email address as the local ID. The *email-string* argument is a case-sensitive string of 1 to 255 characters in the format defined by RFC 822, such as sec@abc.com.

fqdn *fqdn-name*: Uses an FQDN as the local ID. The *fqdn-name* argument is a case-sensitive string of 1 to 255 characters, such as www.test.com.

key-id *key-id-string*: Uses the device's key ID as the local ID. The *key-id-string* argument is a case-sensitive string of 1 to 255 characters, and is usually a vendor-specific string for doing proprietary types of identification.

Usage guidelines

Peers exchange local IDs for identifying each other in negotiation.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

Use IP address 2.2.2.2 as the local ID.

```
[Sysname-ikev2-profile-profile1] identity local address 2.2.2.2
```

Related commands

peer

ikev2 cookie-challenge

Use **ikev2 cookie-challenge** to enable the cookie challenging feature.

Use **undo ikev2 cookie-challenge** to disable the cookie challenging feature.

Syntax

ikev2 cookie-challenge *number*

undo ikev2 cookie-challenge

Default

The cookie challenging feature is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

number: Specifies the threshold for triggering the cookie challenging feature. The value range for this argument is 0 to 1000 half-open IKE SAs.

Usage guidelines

When an IKEv2 responder maintains a threshold number of half-open IKE SAs, it starts the cookie challenging mechanism. The responder generates a cookie and includes it in the response sent to the initiator. If the initiator initiates a new IKE_SA_INIT request that carries the correct cookie, the responder considers the initiator valid and proceeds with the negotiation. If the carried cookie is incorrect, the responder terminates the negotiation.

This feature can protect the responder against DoS attacks which aim to exhaust the responder's system resources by using a large number of IKE_SA_INIT requests with forged source IP addresses.

Examples

Enable the cookie challenging feature and set the threshold to 450.

```
<Sysname> system-view
[Sysname] ikev2 cookie-challenge 450
```

ikev2 dpd

Use **ikev2 dpd** to configure global IKEv2 DPD.

Use **undo ikev2 dpd** to disable global IKEv2 DPD.

Syntax

ikev2 dpd interval *interval* [**retry** *seconds*] { **on-demand** | **periodic** }

undo ikev2 dpd interval

Default

The global IKEv2 DPD feature is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

interval *interval*: Specifies a DPD triggering interval in the range of 10 to 3600 seconds.

retry *seconds*: Specifies the DPD retry interval in the range of 2 to 60 seconds. The default is 5 seconds.

on-demand: Triggers DPD on demand. The device triggers DPD if it has IPsec traffic to send and has not received any IPsec packets from the peer for the specified interval.

periodic: Triggers DPD at regular intervals. The device triggers DPD at the specified interval.

Usage guidelines

DPD is triggered periodically or on-demand. As a best practice, use the on-demand mode when the device communicates with a large number of IKEv2 peers. For an earlier detection of dead peers, use the periodic triggering mode, which consumes more bandwidth and CPU.

The triggering interval must be longer than the retry interval, so that the device will not trigger a new round of DPD during a DPD retry.

You can configure IKEv2 DPD in both IKEv2 profile view and system view. The IKEv2 DPD settings in IKEv2 profile view apply. If you do not configure IKEv2 DPD in IKEv2 profile view, the IKEv2 DPD settings in system view apply.

Examples

Configure the device to trigger IKEv2 DPD if it has IPsec traffic to send and has not received any IPsec packets from the peer for 15 seconds.

```
<Sysname> system-view
[Sysname] ikev2 dpd interval 15 on-demand
```

Configure the device to trigger IKEv2 DPD every 15 seconds.

```
<Sysname> system-view
[Sysname] ikev2 dpd interval 15 periodic
```

Related commands

dpd (IKEv2 profile view)

ikev2 keychain

Use **ikev2 keychain** to create an IKEv2 keychain and enter its view, or enter the view of an existing IKEv2 keychain.

Use **undo ikev2 keychain** to delete an IKEv2 keychain.

Syntax

ikev2 keychain *keychain-name*

undo ikev2 keychain *keychain-name*

Default

No IKEv2 keychains exist.

Views

System view

Predefined user roles

network-admin

Parameters

keychain-name: Specifies a name for the IKEv2 keychain. The keychain name is a case-insensitive string of 1 to 63 characters and cannot contain a hyphen (-).

Usage guidelines

An IKEv2 keychain is required on both ends if either end uses preshared key authentication. The preshared key configured on both ends must be the same.

You can configure multiple IKEv2 peers in an IKEv2 keychain.

Examples

Create an IKEv2 keychain named **key1** and enter IKEv2 keychain view.

```
<Sysname> system-view
[Sysname] ikev2 keychain key1
[Sysname-ikev2-keychain-key1]
```

ikev2 nat-keepalive

Use **ikev2 nat-keepalive** to set the NAT keepalive interval.

Use **undo ikev2 nat-keepalive** to restore the default.

Syntax

ikev2 nat-keepalive *seconds*

undo ikev2 nat-keepalive

Default

The NAT keepalive interval is 10 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

seconds: Specifies the NAT keepalive interval in seconds, in the range of 5 to 3600.

Usage guidelines

This command takes effect when the device resides in the private network behind a NAT device. The device must send NAT keepalive packets regularly to its peer to keep the NAT session alive, so that the peer can access the device.

The NAT keepalive interval must be shorter than the NAT session lifetime.

Examples

Set the NAT keepalive interval to 5 seconds.

```
<Sysname> system-view
[Sysname] ikev2 nat-keepalive 5
```

ikev2 policy

Use **ikev2 policy** to create an IKEv2 policy and enter its view, or enter the view of an existing IKEv2 policy.

Use **undo ikev2 policy** to delete an IKEv2 policy.

Syntax

ikev2 policy *policy-name*

undo ikev2 policy *policy-name*

Default

An IKEv2 policy named **default** exists, which uses the default IKEv2 proposal and matches any local addresses.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a name for the IKEv2 policy. The policy name is a case-insensitive string of 1 to 63 characters.

Usage guidelines

Each end must have an IKEv2 policy for the IKE_SA_INIT exchange. The initiator looks up an IKEv2 policy by the IP address of the interface to which the IPsec policy is applied. The responder looks up an IKEv2 policy by the IP address of the interface that receives the IKEv2 packet. An IKEv2 policy uses IKEv2 proposals to define the encryption algorithms, integrity protection algorithms, PRF algorithms, and DH groups to be used for negotiation.

You can configure multiple IKEv2 policies. An IKEv2 policy must have a minimum of one IKEv2 proposal. Otherwise, the policy is incomplete.

If the initiator uses an IPsec policy that is bound to a source interface, the initiator looks up an IKEv2 policy by the IP address of the source interface.

You can set priorities to adjust the match order of IKEv2 policies that have the same match criteria.

If no IKEv2 policy is configured, the default IKEv2 policy is used. You cannot enter the view of the default IKEv2 policy, nor modify it.

Examples

Create an IKEv2 policy named **policy1** and enter IKEv2 policy view.

```
<Sysname> system-view
[Sysname] ikev2 policy policy1
[Sysname-ikev2-policy-policy1]
```

Related commands

display ikev2 policy

ikev2 profile

Use **ikev2 profile** to create an IKEv2 profile and enter its view, or enter the view of an existing IKEv2 profile.

Use **undo ikev2 profile** to delete an IKEv2 profile.

Syntax

ikev2 profile *profile-name*

undo ikev2 profile *profile-name*

Default

No IKEv2 profiles exist.

Views

System view

Predefined user roles

network-admin

Parameters

profile-name: Specifies a name for the IKEv2 profile. The profile name is a case-insensitive string of 1 to 63 characters.

Usage guidelines

An IKEv2 profile contains the IKEv2 SA parameters that are not negotiated, such as the identity information and authentication methods of the peers, and the matching criteria for profile lookup.

Examples

Create an IKEv2 profile named **profile1** and enter IKEv2 profile view.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
[Sysname-ikev2-profile-profile1]
```

Related commands

display ikev2 profile

ikev2 proposal

Use **ikev2 proposal** to create an IKEv2 proposal and enter its view, or enter the view of an existing IKEv2 proposal.

Use **undo ikev2 proposal** to delete an IKEv2 proposal.

Syntax

ikev2 proposal *proposal-name*

undo ikev2 proposal *proposal-name*

Default

An IKEv2 proposal named **default** exists.

The default IKEv2 proposal has the lowest priority and uses the following settings in non-FIPS mode:

- **Encryption algorithm**—AES-CBC-128 and 3DES.
- **Integrity protection algorithm**—HMAC-SHA1 and HMAC-MD5.
- **PRF algorithm**—HMAC-SHA1 and HMAC-MD5.
- **DH group**—Group 5 and group 2.

The default IKEv2 proposal has the lowest priority and uses the following settings in FIPS mode:

- **Encryption algorithm**—AES-CBC-128 and AES-CTR-128.
- **Integrity protection algorithm**—HMAC-SHA1 and HMAC-SHA256.
- **PRF algorithm**—HMAC-SHA1 and HMAC-SHA256.
- **DH group**—Group 14 and group 19.

Views

System view

Predefined user roles

network-admin

Parameters

proposal-name: Specifies a name for the IKEv2 proposal. The proposal name is a case-insensitive string of 1 to 63 characters and cannot be **default**.

Usage guidelines

An IKEv2 proposal contains security parameters used in IKE_SA_INIT exchanges, including the encryption algorithms, integrity protection algorithms, PRF algorithms, and DH groups.

An IKEv2 proposal must have a minimum of one set of security parameters, including one encryption algorithm, one integrity protection algorithm, one PRF algorithm, and one DH group.

In an IKEv2 proposal, you can specify multiple parameters of the same type. The parameters of different types combine and form multiple sets of security parameters. If you want to use only one set of security parameters, configure only one set of security parameters for the IKEv2 proposal.

Examples

Create an IKEv2 proposal named **prop1**. Specify encryption algorithm AES-CBC-128, integrity protection algorithm SHA1, PRF algorithm SHA1, and DH group 2.

```
<Sysname> system-view
[Sysname] ikev2 proposal prop1
[Sysname-ikev2-proposal-prop1] encryption aes-cbc-128
[Sysname-ikev2-proposal-prop1] integrity sha1
[Sysname-ikev2-proposal-prop1] prf sha1
```

```
[Sysname-ikev2-proposal-prop1] dh group2
```

Related commands

encryption-algorithm

integrity

prf

dh

integrity

Use **integrity** to specify integrity protection algorithms for an IKEv2 proposal.

Use **undo integrity** to restore the default.

Syntax

In non-FIPS mode:

integrity { **aes-xcbc-mac** | **md5** | **sha1** | **sha256** | **sha384** | **sha512** } *

undo integrity

In FIPS mode:

integrity { **sha1** | **sha256** | **sha384** | **sha512** } *

undo integrity

Default

No integrity protection algorithm is specified for an IKEv2 proposal.

Views

IKEv2 proposal view

Predefined user roles

network-admin

Parameters

aes-xcbc-mac: Uses the HMAC-AES-XCBC-MAC algorithm.

md5: Uses the HMAC-MD5 algorithm.

sha1: Uses the HMAC-SHA1 algorithm.

sha256: Uses the HMAC-SHA256 algorithm.

sha384: Uses the HMAC-SHA384 algorithm.

sha512: Uses the HMAC-SHA512 algorithm.

Usage guidelines

You must specify a minimum of one integrity protection algorithm for an IKEv2 proposal. Otherwise, the proposal is incomplete and useless. You can specify multiple integrity protection algorithms for an IKEv2 proposal. An algorithm specified earlier has a higher priority.

Examples

Create an IKEv2 proposal named **prop1**.

```
<Sysname> system-view
[Sysname] ikev2 proposal prop1
```

Specify HMAC-SHA1 and HMAC-MD5 as the integrity protection algorithms, with HMAC-SHA1 preferred.

```
[Sysname-ikev2-proposal-prop1] integrity sha1 md5
```

Related commands

ikev2 proposal

keychain

Use **keychain** to specify an IKEv2 keychain for preshared key authentication.

Use **undo keychain** to restore the default.

Syntax

keychain *keychain-name*

undo keychain

Default

No IKEv2 keychain is specified for an IKEv2 profile.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

keychain-name: Specifies an IKEv2 keychain by its name. The keychain name is a case-insensitive string of 1 to 63 characters and cannot contain a hyphen (-).

Usage guidelines

An IKEv2 keychain is required on both ends if either end uses preshared key authentication. You can specify only one IKEv2 keychain for an IKEv2 profile.

You can specify the same IKEv2 keychain for different IKEv2 profiles.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

Specify IKEv2 keychain **keychain1**.

```
[Sysname-ikev2-profile-profile1] keychain keychain1
```

Related commands

display ikev2 profile

ikev2 keychain

match local (IKEv2 profile view)

Use **match local** to specify a local interface or a local IP address to which an IKEv2 profile can be applied.

Use **undo match local** to remove a local interface or a local IP address to which an IKEv2 profile can be applied.

Syntax

match local address { *interface-type interface-number* | *ipv4-address* | **ipv6** *ipv6-address* }

undo match local address { *interface-type interface-number* | *ipv4-address* | **ipv6** *ipv6-address* }

Default

An IKEv2 profile can be applied to any local interface or IP address.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

address: Specifies a local interface or IP address to which an IKEv2 profile can be applied.

interface-type interface-number: Specifies a local interface by its type and number. It can be any Layer 3 interface.

ipv4-address: Specifies the IPv4 address of a local interface.

ipv6 *ipv6-address*: Specifies the IPv6 address of a local interface.

Usage guidelines

Use this command to specify which address or interface can use the IKEv2 profile for IKEv2 negotiation. The interface is the interface that receives IKEv2 packets. The IP address is the IP address of the interface that receives IKEv2 packets.

An IKEv2 profile configured earlier has a higher priority. To give an IKEv2 profile that is configured later a higher priority, you can configure the **priority** command or this command for the profile. For example, suppose you configured IKEv2 profile A before configuring IKEv2 profile B, and you configured the **match remote identity address range 2.2.2.1 2.2.2.100** command for IKEv2 profile A and the **match remote identity address range 2.2.2.1 2.2.2.10** command for IKEv2 profile B. For the local interface with the IP address 3.3.3.3 to negotiate with the peer 2.2.2.6, IKEv2 profile A is preferred because IKEv2 profile A was configured earlier. To use IKEv2 profile B, you can use this command to restrict the application scope of IKEv2 profile B to IPv4 address 3.3.3.3.

You can specify multiple applicable local interfaces or IP addresses for an IKEv2 profile.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

Apply IKEv2 profile **profile1** to the interface whose IP address is 2.2.2.2.

```
[Sysname-ikev2-profile-profile1] match local address 2.2.2.2
```

Related commands

match remote

match local address (IKEv2 policy view)

Use **match local address** to specify a local interface or a local address that an IKEv2 policy matches.

Use **undo match local address** to remove a local interface or a local address that an IKEv2 policy matches.

Syntax

match local address { *interface-type interface-number* | *ipv4-address* | **ipv6** *ipv6-address* }

undo match local address { *interface-type interface-number* | *ipv4-address* | **ipv6** *ipv6-address* }

Default

No local interface or local address is specified, and the IKEv2 policy matches any local interface or local address.

Views

IKEv2 policy view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies a local interface by its type and number. It can be any Layer 3 interface.

ipv4-address: Specifies the IPv4 address of a local interface.

ipv6 *ipv6-address*: Specifies the IPv6 address of a local interface.

Usage guidelines

IKEv2 policies with this command configured are looked up before those that do not have this command configured.

Examples

Configure IKEv2 policy **policy1** to match local address 3.3.3.3.

```
<Sysname> system-view
[Sysname] ikev2 policy policy1
[Sysname-ikev2-policy-policy1] match local address 3.3.3.3
```

Related commands

display ikev2 policy

match remote

Use **match remote** to configure a peer ID that an IKEv2 profile matches.

Use **undo match remote** to delete a peer ID that an IKEv2 profile matches.

Syntax

match remote { **certificate** *policy-name* | **identity** { **address** { { *ipv4-address* [*mask* | *mask-length*] | **range** *low-ipv4-address high-ipv4-address* } | **ipv6** { *ipv6-address* [*prefix-length*] | **range** *low-ipv6-address high-ipv6-address* } } | **fqdn** *fqdn-name* | **email** *email-string* | **key-id** *key-id-string* } }

undo match remote { **certificate** *policy-name* | **identity** { **address** { { *ipv4-address* [*mask* |*mask-length*] | **range** *low-ipv4-address high-ipv4-address* } | **ipv6** { *ipv6-address* [*prefix-length*] | **range**

low-ipv6-address high-ipv6-address } } | **fqdn** *fqdn-name* | **email** *email-string* | **key-id** *key-id-string* } }

Default

No matching peer ID is configured for the IKEv2 profile.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

certificate *policy-name*: Uses the information in the peer's digital certificate as the peer ID for IKEv2 profile matching. The *policy-name* argument specifies a certificate-based access control policy by its name, a case-insensitive string of 1 to 31 characters.

identity: Uses the specified information as the peer ID for IKEv2 profile matching. The specified information is configured on the peer by using the **identity local** command.

- **address** *ipv4-address* [*mask* | *mask-length*]: Uses an IPv4 host address or an IPv4 subnet address as the peer ID for IKEv2 profile matching. The value range for the *mask-length* argument is 0 to 32. If you do not specify a mask or mask length, the 32-bit mask is used.
- **address range** *low-ipv4-address high-ipv4-address*: Uses a range of IPv4 addresses as the peer ID for IKEv2 profile matching. The end address must be higher than the start address.
- **address ipv6** *ipv6-address* [*prefix-length*]: Uses an IPv6 host address or an IPv6 subnet address as the peer ID for IKEv2 profile matching. The value range for the *prefix-length* argument is 0 to 128. If you do not specify a prefix length, the 128-bit prefix is used.
- **address ipv6 range** *low-ipv6-address high-ipv6-address*: Uses a range of IPv6 addresses as the peer ID for IKEv2 profile matching. The end address must be higher than the start address.
- **fqdn** *fqdn-name*: Uses the peer's FQDN as the peer ID for IKEv2 profile matching. The *fqdn-name* argument is a case-sensitive string of 1 to 255 characters, such as www.test.com.
- **email** *email-string*: Uses peer's email address as the peer ID for IKEv2 profile matching. The *email-string* argument is a case-sensitive string of 1 to 255 characters in the format defined by RFC 822, such as sec@abc.com.
- **key-id** *key-id-string*: Uses the peer's key ID as the peer ID for IKEv2 profile matching. The *key-id-string* argument is a case-sensitive string of 1 to 255 characters, and is usually a vendor-specific string for doing proprietary types of identification.

Usage guidelines

The device compares the received peer ID with the peer IDs configured in local IKEv2 profiles. If a match is found, it uses the IKEv2 profile with the matching peer ID for IKEv2 negotiation.

If the device has the **match remote** and **match local address** commands configured, it uses the IKEv2 profile that matches all the criteria configured by the commands.

To make sure only one IKEv2 profile is matched for a peer, do not configure the same peer ID for two or more IKEv2 profiles. If you configure the same peer ID for two or more IKEv2 profiles, which IKEv2 profile is selected for IKEv2 negotiation is unpredictable.

You can configure an IKEv2 profile to match multiple peer IDs. A peer ID configured earlier has a higher priority.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

Configure the IKEv2 profile to match the peer ID that is FQDN name **www.test.com**.

```
[Sysname-ikev2-profile-profile1] match remote identity fqdn www.test.com
```

Configure the IKEv2 profile to match the peer ID that is IP address 10.1.1.1.

```
[Sysname-ikev2-profile-profile1]match remote identity address 10.1.1.1
```

Related commands

identity local

match local address

nat-keepalive

Use **nat-keepalive** to set the NAT keepalive interval.

Use **undo nat-keepalive** to restore the default.

Syntax

nat-keepalive *seconds*

undo nat-keepalive

Default

The NAT keepalive interval set in system view is used.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

seconds: Specifies the NAT keepalive interval in seconds, in the range of 5 to 3600.

Usage guidelines

This command takes effect when the device resides in the private network behind a NAT device. The device must send NAT keepalive packets regularly to its peer to keep the NAT session alive, so that the peer can access the device.

The NAT keepalive interval must be shorter than the NAT session lifetime.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

Set the NAT keepalive interval to 1200 seconds.

```
[Sysname-ikev2-profile-profile1]nat-keepalive 1200
```

Related commands

display ikev2 profile

ikev2 nat-keepalive

peer

Use **peer** to create an IKEv2 peer and enter its view, or enter the view of an existing IKEv2 peer.

Use **undo peer** to delete an IKEv2 peer.

Syntax

peer *name*

undo peer *name*

Default

No IKEv2 peers exist.

Views

IKEv2 keychain view

Predefined user roles

network-admin

Parameters

name: Specifies a name for the IKEv2 peer. The peer name is a case-insensitive string of 1 to 63 characters.

Usage guidelines

An IKEv2 peer contains a preshared key and the criteria for looking up the peer. The criteria for peer lookup includes the peer's host name, IP address, IP address range, and ID. The IKEv2 negotiation initiator uses the peer's host name, IP address, or IP address range to look up its peer. The responder uses the peer's IP address, IP address range, or ID to look up its peer.

Examples

Create an IKEv2 keychain named **key1** and enter IKEv2 keychain view.

```
<Sysname> system-view
[Sysname] ikev2 keychain key1
```

Create an IKEv2 peer named **peer1**.

```
[Sysname-ikev2-keychain-key1] peer peer1
```

Related commands

address

hostname

identity

ikev2 keychain

pre-shared-key

Use **pre-shared-key** to configure a preshared key.

Use **undo pre-shared-key** to delete a preshared key.

Syntax

pre-shared-key [**local** | **remote**] { **ciphertext** | **plaintext** } *string*

undo pre-shared-key [**local** | **remote**]

Default

No preshared key exists.

Views

IKEv2 peer view

Predefined user roles

network-admin

Parameters

`local`: Specifies a preshared key for certificate signing.

`remote`: Specifies a preshared key for certificate authentication.

`ciphertext`: Specifies a preshared key in encrypted form.

`plaintext`: Specifies a preshared key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

`string`: Specifies the preshared key. The key is case sensitive. In non-FIPS mode, its plaintext form is a string of 1 to 128 characters and its encrypted form is a string of 1 to 201 characters. In FIPS mode, its plaintext form is a string of 15 to 128 characters and its encrypted form is a string of 15 to 201 characters.

Usage guidelines

If you specify the **`local`** or **`remote`** keyword, you configure an asymmetric key. If you specify neither the **`local`** nor the **`remote`** keyword, you configure a symmetric key.

To delete a key by using the **undo** command, you must specify the correct key type. For example, if you configure a key by using the **`pre-shared-key local`** command, you cannot delete the key by using the **`undo pre-shared-key`** or **`undo pre-shared-key remote`** command.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

- On the initiator:

  # Create an IKEv2 keychain named **key1**.

  ```
  <Sysname> system-view
  [Sysname] ikev2 keychain key1
  ```

  # Create an IKEv2 peer named **peer1**.

  ```
  [Sysname-ikev2-keychain-key1] peer peer1
  ```

  # Configure **111-key** as the symmetric plaintext preshared key.

  ```
  [Sysname-ikev2-keychain-key1-peer-peer1] pre-shared-key plaintext 111-key
  [Sysname-ikev2-keychain-key1-peer-peer1] quit
  ```

  # Create an IKEv2 peer named **peer2**.

  ```
  [Sysname-ikev2-keychain-key1] peer peer2
  ```

  # Configure asymmetric plaintext preshared keys. The key for certificate signing is **111-key-a** and the key for certificate authentication is **111-key-b**.

  ```
  [Sysname-ikev2-keychain-key1-peer-peer2] pre-shared-key local plaintext 111-key-a
  [Sysname-ikev2-keychain-key1-peer-peer2] pre-shared-key remote plaintext 111-key-b
  ```

- On the responder:

  # Create an IKEv2 keychain named **telecom**.

  ```
  <Sysname> system-view
  [Sysname] ikev2 keychain telecom
  ```

  # Create an IKEv2 peer named **peer1**.

```
[Sysname-ikev2-keychain-telecom] peer peer1
```

Configure **111-key** as the symmetric plaintext preshared key.

```
[Sysname-ikev2-keychain-telecom-peer-peer1] pre-shared-key plaintext 111-key
[Sysname-ikev2-keychain-telecom-peer-peer1] quit
```

Create an IKEv2 peer named **peer2**.

```
[Sysname-ikev2-keychain-telecom] peer peer2
```

Configure asymmetric plaintext preshared keys. The key for certificate signing is **111-key-b** and the key for certificate authentication is **111-key-a**.

```
[Sysname-ikev2-keychain-telecom-peer-peer2] pre-shared-key local plaintext
111-key-b
[Sysname-ikev2-keychain-telecom-peer-peer2] pre-shared-key remote plaintext
111-key-a
```

Related commands

ikev2 keychain

peer

prf

Use **prf** to specify pseudo-random function (PRF) algorithms for an IKEv2 proposal.

Use **undo prf** to restore the default.

Syntax

In non-FIPS mode:

prf { **aes-xcbc-mac** | **md5** | **sha1** | **sha256** | **sha384** | **sha512** } *

undo prf

In FIPS mode:

prf { **sha1** | **sha256** | **sha384** | **sha512** } *

undo prf

Default

An IKEv2 proposal uses the integrity protection algorithms as the PRF algorithms.

Views

IKEv2 proposal view

Predefined user roles

network-admin

Parameters

aes-xcbc-mac: Uses the HMAC-AES-XCBC-MAC algorithm.

md5: Uses the HMAC-MD5 algorithm.

sha1: Uses the HMAC-SHA1 algorithm.

sha256: Uses the HMAC-SHA256 algorithm.

sha384: Uses the HMAC-SHA384 algorithm.

sha512: Uses the HMAC-SHA512 algorithm.

Usage guidelines

You can specify multiple PRF algorithms for an IKEv2 proposal. An algorithm specified earlier has a higher priority.

Examples

Create an IKEv2 proposal named **prop1**.

```
<Sysname> system-view
[Sysname] ikev2 proposal prop1
```

Specify HMAC-SHA1 and HMAC-MD5 as the PRF algorithms, with HMAC-SHA1 preferred.

```
[Sysname-ikev2-proposal-prop1] prf sha1 md5
```

Related commands

ikev2 proposal

integrity

priority (IKEv2 policy view)

Use **priority** to set a priority for an IKEv2 policy.

Use **undo priority** to restore the default.

Syntax

priority *priority*

undo priority

Default

The priority of an IKEv2 policy is 100.

Views

IKEv2 policy view

Predefined user roles

network-admin

Parameters

priority: Specifies the priority of the IKEv2 policy, in the range of 1 to 65535. A smaller number represents a higher priority.

Usage guidelines

The priority set by this command can only be used to adjust the match order of IKEv2 policies.

Examples

Set the priority to 10 for IKEv2 policy **policy1**.

```
<Sysname> system-view
[Sysname] ikev2 policy policy1
[Sysname-ikev2-policy-policy1] priority 10
```

Related commands

display ikev2 policy

priority (IKEv2 profile view)

Use **priority** to set a priority for an IKEv2 profile.

Use **undo priority** to restore the default.

Syntax

priority *priority*

undo priority

Default

The priority of an IKEv2 profile is 100.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

priority: Specifies the priority of the IKEv2 profile, in the range of 1 to 65535. A smaller number represents a higher priority.

Usage guidelines

The priority set by this command can only be used to adjust the match order of IKEv2 profiles.

Examples

Set the priority to 10 for IKEv2 profile **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
[Sysname-ikev2-profile-profile1] priority 10
```

proposal

Use **proposal** to specify an IKEv2 proposal for an IKEv2 policy.

Use **undo proposal** to remove an IKEv2 proposal from an IKEv2 policy.

Syntax

proposal *proposal-name*

undo proposal *proposal-name*

Default

No IKEv2 proposal is specified for an IKEv2 policy.

Views

IKEv2 policy view

Predefined user roles

network-admin

Parameters

proposal-name: Specifies an IKEv2 proposal by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can specify multiple IKEv2 proposals for an IKEv2 policy. A proposal specified earlier has a higher priority.

Examples

Specify IKEv2 proposal **proposal1** for IKEv2 policy **policy1**.

```
<Sysname> system-view
[Sysname] ikev2 policy policy1
[Sysname-ikev2-policy-policy1] proposal proposal1
```

Related commands

display ikev2 policy

ikev2 proposal

reset ikev2 sa

Use **reset ikev2 sa** to delete IKEv2 SAs.

Syntax

reset ikev2 sa [[{ **local** | **remote** } { *ipv4-address* | **ipv6** *ipv6-address* }] | **tunnel** *tunnel-id*] [**fast**]

Views

User view

Predefined user roles

network-admin

Parameters

local: Deletes IKEv2 SAs for a local IP address.

remote: Deletes IKEv2 SAs for a remote IP address.

ipv4-address: Specifies a local or remote IPv4 address.

ipv6 *ipv6-address*: Specifies a local or remote IPv6 address.

tunnel *tunnel-id*: Deletes IKEv2 SAs for an IPsec tunnel. The *tunnel-id* argument specifies an IPsec tunnel by its ID in the range of 1 to 2000000000.

fast: Notifies the peers of the deletion and deletes IKEv2 SAs directly before receiving the peers' responses. If you do not specify this keyword, the device notifies the peers of the deletion and deletes IKEv2 SAs after it receives the peers' responses.

Usage guidelines

Deleting an IKEv2 SA will also delete the child SAs negotiated through the IKEv2 SA.

If you do not specify any parameters, this command deletes all IKEv2 SAs and the child SAs negotiated through the IKEv2 SAs.

Examples

Display information about IKEv2 SAs.

```
<Sysname> display ikev2 sa
     Tunnel ID          Local             Remote             Status
  ------------------------------------------------------------------------
     1                  1.1.1.1/500       1.1.1.2/500        EST
     2                  2.2.2.1/500       2.2.2.2/500        EST
  Status:
  IN-NEGO: Negotiating, EST: Established, DEL: Deleting
```

Delete the IKEv2 SA whose remote IP address is 1.1.1.2.

```
<Sysname> reset ikev2 sa remote 1.1.1.2
```

Display information about IKEv2 SAs again. Verify that the IKEv2 SA is deleted.

```
<Sysname> display ikev2 sa
     Tunnel ID          Local             Remote             Status
  ------------------------------------------------------------------------
     2                  2.2.2.1/500       2.2.2.2/500        EST
  Status:
  IN-NEGO: Negotiating, EST: Established, DEL: Deleting
```

Related commands

display ikev2 sa

reset ikev2 statistics

Use **reset ikev2 statistics** to clear IKEv2 statistics.

Syntax

reset ikev2 statistics

Views

User view

Predefined user roles

network-admin

Examples

Clear IKEv2 statistics.

```
<Sysname> reset ikev2 statistics
```

Related commands

display ikev2 statistics

sa duration

Use **sa duration** to set the IKEv2 SA lifetime.

Use **undo sa duration** to restore the default.

Syntax

sa duration *seconds*

undo sa duration

Default

The IKEv2 SA lifetime is 86400 seconds.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

seconds: Specifies the IKEv2 SA lifetime in seconds, in the range of 120 to 86400.

Usage guidelines

An IKEv2 SA can be used for subsequent IKEv2 negotiations before its lifetime expires, saving a lot of negotiation time. However, the longer the lifetime, the higher the possibility that attackers collect enough information and initiate attacks.

Two peers can have different IKEv2 SA lifetime settings, and they do not perform lifetime negotiation. The peer with a shorter lifetime always initiates the rekeying.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
```

Set the IKEv2 SA lifetime to 1200 seconds.

```
[Sysname-ikev2-profile-profile1] sa duration 1200
```

Related commands

display ikev2 profile

Contents

SSH commands

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

SSH server commands

display ssh server

Use **display ssh server** on an SSH server to display the SSH server status or sessions.

Syntax

display ssh server { **session** | **status** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

session: Specifies the SSH server sessions.

status: Specifies the SSH server status.

Examples

Display the SSH server status.

```
<Sysname> display ssh server status
 Stelnet server: Disable
 SSH version : 2.0
 SSH authentication-timeout : 60 second(s)
 SSH server key generating interval : 0 hour(s)
 SSH authentication retries : 3 time(s)
 SFTP server: Disable
 SFTP server Idle-Timeout: 10 minute(s)
 NETCONF server: Disable
 SCP server: Disable
 SSH Server PKI domain name: aaa
```

Table 1 Command output

Field	Description
Stelnet server	Whether the Stelnet server is enabled.
SSH version	SSH protocol version. When the SSH supports SSH1, the protocol version is 1.99. Otherwise, the protocol version is 2.
SSH authentication-timeout	Authentication timeout timer.

Field	Description
SSH server key generating interval	Minimum interval for updating the RSA server key pair.
SSH authentication retries	Maximum number of authentication attempts for SSH users.
SFTP server	Whether the SFTP server is enabled.
SFTP server Idle-Timeout	SFTP connection idle timeout timer.
NETCONF server	Whether NETCONF over SSH is enabled.
SCP server	Whether the SCP server is enabled.
SSH Server PKI domain name	Name of the PKI domain specified for the SSH server.

Display the SSH server sessions.

```
<Sysname> display ssh server session
UserPid   SessID Ver   Encrypt    State          Retries  Serv     Username
 184       0     2.0   aes128-cbc Established    1        Stelnet  abc@123
```

Table 2 Command output

Field	Description
UserPid	User process ID.
SessID	Session ID.
Ver	Protocol version of the SSH server.
Encrypt	Encryption algorithm used on the SSH server.
State	Session state: • **Init**—Initialization. • **Ver-exchange**—Version negotiation. • **Keys-exchange**—Key exchange. • **Auth-request**—Authentication request. • **Serv-request**—Session service request. • **Established**—The session is established. • **Disconnected**—The session is terminated.
Retries	Number of authentication failures.
Serv	Service type: • SCP. • SFTP. • Stelnet. • NETCONF.
Username	Username that the client uses to log in to the server.

display ssh user-information

Use **display ssh user-information** to display information about SSH users on an SSH server.

Syntax

display ssh user-information [*username*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

username: Specifies an SSH username, a case-sensitive string of 1 to 80 characters. If you do not specify an SSH user, this command displays information about all SSH users.

Usage guidelines

This command displays information only about SSH users that are configured by using the **ssh user** command on the SSH server.

Examples

Display information about all SSH users.

```
<Sysname> display ssh user-information
 Total ssh users:2
 Username            Authentication-type  User-public-key-name  Service-type
 yemx                password                                   Stelnet|SFTP
 test                publickey            pubkey                SFTP
```

Table 3 Command output

Field	Description
Total ssh users	Total number of SSH users.
Authentication-type	Authentication methods: • Password authentication. • Publickey authentication. • Password-publickey authentication. • Any authentication.
User-public-key-name	Public key name of the user. This field is empty if the authentication method is password authentication.
Service-type	Service types: • Stelnet. • SFTP. • SCP. • NETCONF. If multiple service types are available for an SSH user, they are separated by vertical bars (|).

Related commands

ssh user

free ssh

Use **free ssh** to disconnect SSH sessions.

Syntax

free ssh { **user-ip** { *ip-address* | **ipv6** *ipv6-address* } [**port** *port-number*] | **user-pid** *pid-number* | **username** *username* }

Views

User view

Predefined user roles

network-admin

Parameters

user-ip: Specifies the user IP address of the SSH sessions to be disconnected.

ip-address: Specifies the user IPv4 address of the SSH sessions to be disconnected.

ipv6 *ipv6-address:* Specifies the user IPv6 address of the SSH sessions to be disconnected.

port *port-number*: Specifies the source port of the SSH session to be disconnected, in the range of 1 to 65535. If you do not specify a source port, this command disconnects all SSH sessions using the specified IP address.

user-pid *pid-number*: Specifies the user process ID of the SSH session to be disconnected, in the range of 1 to 2147483647. To view the user process ID of an SSH session, use the **display ssh server session** command.

username *username*: Specifies the username of the SSH session to be disconnected. To view the username of an SSH session, use the **display ssh server session** command.

Examples

Disconnect the SSH sessions with user IPv4 address 192.168.15.45.

```
<Sysname> free ssh user-ip 192.168.15.45
Releasing SSH connection. Continue? [Y/N]:y
```

Disconnect the SSH sessions with user IPv6 address 2000::11.

```
<Sysname> free ssh user-ip ipv6 2000::11
Releasing SSH connection. Continue? [Y/N]:y
```

Disconnect the SSH session with user process ID 417.

```
<Sysname> free ssh user-pid 417
Releasing SSH connection. Continue? [Y/N]:y
```

Disconnect the SSH session with username **sshuser**.

```
<Sysname> free ssh username sshuser
Releasing SSH connection. Continue? [Y/N]:y
```

Related commands

display ssh server session

scp server enable

Use **scp server enable** to enable the SCP server.

Use **undo scp server enable** to disable the SCP server.

Syntax

scp server enable

undo scp server enable

Default

The SCP server is disabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable the SCP server.

```
<Sysname> system-view
[Sysname] scp server enable
```

Related commands

display ssh server

sftp server enable

Use **sftp server enable** to enable the SFTP server.

Use **undo sftp server enable** to disable the SFTP server.

Syntax

sftp server enable

undo sftp server enable

Default

The SFTP server is disabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable the SFTP server.

```
<Sysname> system-view
[Sysname] sftp server enable
```

Related commands

display ssh server

sftp server idle-timeout

Use **sftp server idle-timeout** to set the idle timeout timer for SFTP connections on an SFTP server.

Use **undo sftp server idle-timeout** to restore the default.

Syntax

sftp server idle-timeout *time-out-value*

undo sftp server idle-timeout

Default

The idle timeout timer is 10 minutes for SFTP connections.

Views

System view

Predefined user roles

network-admin

Parameters

time-out-value: Specifies an idle timeout timer in the range of 1 to 35791 minutes.

Usage guidelines

If an SFTP connection is idle when the idle timeout timer expires, the system automatically terminates the connection. To promptly release connection resources, set the idle timeout timer to a small value when many SFTP connections concurrently exist.

Examples

Set the idle timeout timer to 500 minutes for SFTP connections.

```
<Sysname> system-view
[Sysname] sftp server idle-timeout 500
```

Related commands

display ssh server

ssh server acl

Use **ssh server acl** to specify an ACL to control IPv4 SSH connections to the server.

Use **undo ssh server acl** to restore the default.

Syntax

ssh server acl { *advanced-acl-number* | *basic-acl-number* | **mac** *mac-acl-number* }

undo ssh server acl

Default

No ACLs are specified and all IPv4 SSH clients can initiate SSH connections to the server.

Views

System view

Predefined user roles

network-admin

Parameters

advanced-acl-number: Specifies an IPv4 advanced ACL number in the range of 3000 to 3999.

basic-acl-number: Specifies an IPv4 basic ACL number in the range of 2000 to 2999.

mac *mac-acl-number:* Specifies a Layer 2 ACL by its number in the range of 4000 to 4999.

Usage guidelines

The ACL specified in this command filters IPv4 SSH clients' connection requests. Only the IPv4 SSH clients that the ACL permits can access the device. If the specified ACL does not exist or contains no rules, all IPv4 SSH clients can access the device.

The ACL takes effect only on SSH connections that are initiated after the ACL configuration.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure ACL 2001 and permit only the users at 1.1.1.1 to initiate SSH connections to the server.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] ssh server acl 2001
```

Related commands

display ssh server

ssh server acl-deny-log enable

Use **ssh server acl-deny-log enable** to enable logging for SSH login attempts that are denied by the SSH login control ACL.

Use **undo ssh server acl-deny-log enable** to disable logging for SSH login attempts that are denied by the SSH login control ACL.

Syntax

ssh server acl-deny-log enable

undo ssh server acl-deny-log enable

Default

Logging is disabled for SSH login attempts that are denied by the SSH login control ACL.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Only SSH clients permitted by the SSH login control ACL can access the SSH server. The logging feature generates log messages for SSH login attempts that are denied by the SSH login control ACL, and sends the messages to the information center.

For information about log message output, see the information center in *Network Management and Monitoring Configuration Guide*. For information about configuring an SSH login control ACL, see the **ssh server acl** or **ssh server ipv6 acl** command.

Examples

Enable logging for SSH login attempts that are denied by the SSH login control ACL.

```
<Sysname> system-view
[Sysname] ssh server acl-deny-log enable
```

Related commands

ssh server acl

ssh server ipv6 acl

ssh server authentication-retries

Use **ssh server authentication-retries** to set the maximum number of authentication attempts for SSH users.

Use **undo ssh server authentication-retries** to restore the default.

Syntax

ssh server authentication-retries *retries*

undo ssh server authentication-retries

Default

The maximum number of authentication attempts is 3 for SSH users.

Views

System view

Predefined user roles

network-admin

Parameters

retries: Specifies the maximum number of authentication attempts for SSH users, in the range of 1 to 5.

Usage guidelines

Setting the maximum number of authentication attempts prevents malicious hacking of usernames and passwords.

If the total number of authentication attempts exceeds the upper limit specified in this command, further authentication is not allowed.

- For **any** authentication, an authentication attempt is a publickey or password authentication process.
- For **password-publickey** authentication, an authentication attempt contains both a publickey authentication process and a password authentication process. The server first uses publickey authentication, and then uses password authentication to authenticate the SSH user.

This configuration does not affect logged-in users. It affects only users that attempt to log in after the configuration.

Examples

Set the maximum number of authentication attempts to 4 for SSH users.

```
<Sysname> system-view
[Sysname] ssh server authentication-retries 4
```

Related commands

display ssh server

ssh server authentication-timeout

Use **ssh server authentication-timeout** to set the SSH user authentication timeout timer on the SSH server.

Use **undo ssh server authentication-timeout** to restore the default.

Syntax

ssh server authentication-timeout *time-out-value*

undo ssh server authentication-timeout

Default

The SSH user authentication timeout timer is 60 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

time-out-value: Specifies an authentication timeout timer in the range of 1 to 120 seconds.

Usage guidelines

If a user does not finish the authentication when the timeout timer expires, the connection cannot be established.

To prevent malicious occupation of TCP connections, set the authentication timeout timer to a small value.

Examples

Set the authentication timeout timer to 10 seconds for SSH users.

```
<Sysname> system-view
[Sysname] ssh server authentication-timeout 10
```

Related commands

display ssh server

ssh server compatible-ssh1x enable

Use **ssh server compatible-ssh1x enable** to enable the SSH server to support SSH1 clients.

Use **undo ssh server compatible-ssh1x** [**enable**] to restore the default.

Syntax

ssh server compatible-ssh1x enable

undo ssh server compatible-ssh1x [**enable**]

Default

The SSH server does not support SSH1 clients.

Views

System view

Predefined user roles

network-admin

network-operator

Usage guidelines

This command is not available in FIPS mode.

The **undo** form of this command restores the default setting whether you specify the **enable** keyword or not.

This configuration does not affect logged-in users. It affects only users that attempt to log in after the configuration.

Examples

Enable the SSH server to support SSH1 clients.

```
<Sysname> system-view
[Sysname] ssh server compatible-ssh1x enable
```

Related commands

display ssh server

ssh server dscp

Use **ssh server dscp** to set the DSCP value in the IPv4 SSH packets that the SSH server sends to SSH clients.

Use **undo ssh server dscp** to restore the default.

Syntax

ssh server dscp *dscp-value*

undo ssh server dscp

Default

The DSCP value is 48 in IPv4 SSH packets.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies the DSCP value in the IPv4 SSH packets, in the range of 0 to 63. A bigger DSCP value represents a higher priority.

Usage guidelines

The DSCP value of a packet specifies the priority of the packet and affects the transmission priority of the packet.

Examples

Set the DSCP value to 30 for IPv4 SSH packets.

```
<Sysname> system-view
[Sysname] ssh server dscp 30
```

ssh server enable

Use **ssh server enable** to enable the Stelnet server.

Use **undo ssh server enable** to disable the Stelnet server.

Syntax

ssh server enable

undo ssh server enable

Default

The Stelnet server is disabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable the Stelnet server.

```
<Sysname> system-view
[Sysname] ssh server enable
```

Related commands

display ssh server

ssh server ipv6 acl

Use **ssh server ipv6 acl** to specify an ACL to control IPv6 SSH connections to the server.

Use **undo ssh server ipv6 acl** to restore the default.

Syntax

ssh server ipv6 acl { **ipv6** { *advanced-acl-number* | *basic-acl-number* } | **mac** *mac-acl-number* }

undo ssh server ipv6 acl

Default

No ACLs are specified and all IPv6 SSH clients can initiate SSH connections to the server.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6: Specifies the IPv6 ACL type.

advanced-acl-number: Specifies an IPv6 advanced ACL number in the range of 3000 to 3999.

basic-acl-number: Specifies an IPv6 basic ACL number in the range of 2000 to 2999.

mac *mac-acl-number:* Specifies a Layer 2 ACL by its number in the range of 4000 to 4999.

Usage guidelines

The ACL specified in this command filters IPv6 SSH clients' connection requests. Only the IPv6 SSH clients that the ACL permits can access the device. If the specified ACL does not exist or contains no rules, all IPv6 SSH clients can access the device.

The ACL takes effect only on SSH connections that are initiated after the ACL configuration.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure ACL 2001 and permit only the users on the subnet 1::1/64 to initiate SSH connections to the server.

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2001
[Sysname-acl6-ipv6-basic-2001] rule permit source 1::1 64
[Sysname-acl6-ipv6-basic-2001] quit
[Sysname] ssh server ipv6 acl ipv6 2001
```

Related commands

display ssh server

ssh server ipv6 dscp

Use **ssh server ipv6 dscp** to set the DSCP value in the IPv6 SSH packets that the SSH server sends to SSH clients.

Use **undo ssh server ipv6 dscp** to restore the default.

Syntax

ssh server ipv6 dscp *dscp-value*

undo ssh server ipv6 dscp

Default

The DSCP value is 48 in IPv6 SSH packets.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies the DSCP value in the IPv6 SSH packets, in the range of 0 to 63. A bigger DSCP value represents a higher priority.

Usage guidelines

The DSCP value of an IPv6 packet specifies the priority of the packet and affects the transmission priority of the packet.

Examples

Set the DSCP value to 30 for IPv6 SSH packets.

```
<Sysname> system-view
[Sysname] ssh server ipv6 dscp 30
```

ssh server key-re-exchange enable

Use **ssh server key-re-exchange enable** to enable SSH algorithm renegotiation and key re-exchange.

Use **undo ssh server key-re-exchange enable** to disable SSH algorithm renegotiation and key re-exchange.

Syntax

ssh server key-re-exchange enable [**interval** *interval*]

undo ssh server key-re-exchange enable

Default

SSH algorithm renegotiation and key re-exchange are disabled.

Views

System view

Predefined user roles

network-admin

Parameters

interval *interval*: Specifies an interval for SSH algorithm renegotiation and key re-exchange, in the range of 1 to 24 hours. If you do not specify this option, the SSH server initiates SSH algorithm renegotiation and key re-exchange at intervals of 1 hour.

Usage guidelines

This command is not available in FIPS mode.

This command enables the SSH server to renegotiate algorithms and re-exchange keys at regular intervals after the first algorithm negotiation and key exchange with SSH clients.

This command takes effect only on new SSH connections that are established after the command is configured, and it does not affect existing SSH connections.

Examples

Enable SSH algorithm renegotiation and key re-exchange.

```
<Sysname> sysname
[Sysname] ssh server key-re-exchange enable
```

ssh server pki-domain

Use **ssh server pki-domain** to specify a PKI domain for an SSH server.

Use **undo ssh server pki-domain** to restore the default.

Syntax

ssh server pki-domain *domain-name*

undo ssh server pki-domain

Default

No PKI domain is specified for an SSH server.

Views

System view

Predefined user roles

network-admin

Parameters

domain-name: Specifies the name of the PKI domain used to verify the SSH server. The PKI domain name is a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

Examples

Specify PKI domain **serverpkidomain** for the SSH server.

```
<Sysname> system-view
```

```
[Sysname] ssh server pki-domain serverpkidomain
```

ssh server port

Use **ssh server port** to specify the SSH service port.

Use **undo ssh server port** to restore the default.

Syntax

ssh server port *port-number*

undo ssh server port

Default

The SSH service port is 22.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies a port number in the range of 1 to 65535.

Usage guidelines

CAUTION:

- If you modify the SSH port number when the SSH server is enabled, the SSH service is restarted and all SSH connections are terminated after the modification. SSH users must reconnect to the SSH server to access the server.
- If you set the SSH port to a well-known port number, the service that uses the well-known port number might fail to start. Well-known port numbers are in the range of 1 to 1024.

Examples

Set the SSH service port to 1025.

```
<Sysname> system-view
[Sysname] ssh server port 1025
```

ssh server rekey-interval

Use **ssh server rekey-interval** to set the minimum interval for updating the RSA server key pair.

Use **undo ssh server rekey-interval** to restore the default.

Syntax

ssh server rekey-interval *interval*

undo ssh server rekey-interval

Default

The minimum interval for updating the RSA server key pair is 0 hours. The system does not update the RSA server key pair.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the minimum interval for updating the RSA server key pair, in the range of 1 to 24 hours.

Usage guidelines

This command is not available in FIPS mode.

Periodically updating the RSA server key pair prevents malicious hacking to the key pair and enhances security of the SSH connections.

The system starts to count down the configured minimum update interval after the first SSH1 user logs in to the server. If a new SSH1 user logs in to the server after the interval, the system performs the following operations:

1. Updates the RSA server key pair.
2. Uses the updated RSA server key pair for key pair negotiation with the new user.
3. Resets the interval and starts to count down the interval again.

This command takes effect only on SSH1 clients.

Examples

Set the minimum interval to 3 hours for updating the RSA server key pair.

```
<Sysname> system-view
[Sysname] ssh server rekey-interval 3
```

Related commands

display ssh server

ssh user

Use **ssh user** to create an SSH user and specify the service type and authentication method.

Use **undo ssh user** to delete an SSH user.

Syntax

In non-FIPS mode:

ssh user *username* **service-type** { **all** | **netconf** | **scp** | **sftp** | **stelnet** } **authentication-type** { **keyboard-interactive** | **password** | { **any** | **password-publickey** | **publickey** } [**assign** { **pki-domain** *domain-name* | **publickey** *keyname*&<1-6> }] }

undo ssh user *username*

In FIPS mode:

ssh user *username* **service-type** { **all** | **netconf** | **scp** | **sftp** | **stelnet** } **authentication-type** { **keyboard-interactive** | **password** | **password-publickey** [**assign** { **pki-domain** *domain-name* | **publickey** *keyname*&<1-6> }] }

undo ssh user *username*

Default

No SSH users exist.

Views

System view

Predefined user roles

network-admin

Parameters

username: Specifies an SSH username, a case-sensitive string of 1 to 80 characters. The username cannot be **a**, **al**, or **all**. In addition, the username cannot include vertical bars (|), colons (:), asterisks (*), question marks (?), or angle brackets (< >). The at sign (@), slash (/), and backslash (\) can only be used to append ISP domain names to usernames in the *pureusername@domain*, *pureusername*/*domain*, and *domain**pureusername* format. Do not include hyphens (-) in the username of an SCP user. Otherwise, SCP logins using that username will fail.

service-type: Specifies a service type for the SSH user.

- **all**: Specifies service types Stelnet, SFTP, SCP, and NETCONF.
- **scp**: Specifies the service type SCP.
- **sftp**: Specifies the service type SFTP.
- **stelnet**: Specifies the service type Stelnet.
- **netconf**: Specifies the service type NETCONF.

authentication-type: Specifies an authentication method for the SSH user.

- **keyboard-interactive**: Specifies keyboard-interactive authentication. This authentication method supports multiple rounds of interactive exchanges of information. To pass authentication, the user must provide all interactive information required by the remote authentication server. If the remote authentication server does not require interactive information, the keyboard-interactive authentication process is the same as the password authentication.
- **password**: Specifies password authentication. This authentication method provides easy and fast encryption, but it is vulnerable. It can work with AAA to implement user authentication, authorization, and accounting.
- **any**: Specifies keyboard-interactive authentication, password authentication, or publickey authentication.
- **password-publickey**: Specifies both password authentication and publickey authentication for SSH2 clients. In SSH2, the password-publickey authentication method provides higher security. If the client runs SSH1, this keyword specifies either password authentication or publickey authentication.
- **publickey**: Specifies publickey authentication. This authentication method has complicated and slow encryption, but it provides strong authentication that can defend against brute-force attacks. This authentication method is easy to use. If this method is configured, the authentication process completes automatically without entering any password.

assign: Specifies parameters used for client verification.

- **pki-domain** *domain-name*: Specifies the PKI domain that verifies the client's digital certificate. The *domain-name* argument is a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes ('). The server uses the CA certificate that is saved in the PKI domain to verify the client's digital certificate. In this scenario, the server does not need to save clients' public keys in advance.

- **publickey** *keyname*&<1-6>: Specifies a space-separated list of up to six SSH client public keys. The *keyname* argument represents the SSH client's public key configured on the server. It is a case-sensitive string of 1 to 64 characters. The server uses the client's public key to check the validity of the client. If the public key file of the client is changed, you must update the client's public key on the server promptly. If you specify multiple client public keys, the device verifies the user identity by using the public keys in the order they are specified. The user is valid if the user passes one public key check.

Usage guidelines

Use this command to configure an SSH user depending on the authentication method.

- If the authentication method is **publickey**, you must create an SSH user and a local user on the SSH server. The two users must have the same username, so that the SSH user can be assigned the correct working directory and user role.
- If the authentication method is **password**, you must perform one of the following tasks:
  - For local authentication, configure a local user on the SSH server.
  - For remote authentication, configure an SSH user on a remote authentication server, for example, a RADIUS server.

  You do not need to create an SSH user by using the **ssh user** command. However, if you want to display all SSH users, including the password-only SSH users, for centralized management, you can use this command to create them. If such an SSH user has been created, make sure you have specified the correct service type and authentication method.
- If the authentication method is **keyboard-interactive**, **password-publickey** or **any**, you must create an SSH user on the SSH server and perform one of the following tasks:
  - For local authentication, configure a local user on the SSH server.
  - For remote authentication, configure an SSH user on a remote authentication server, for example, a RADIUS server.

  In either case, the local user or the SSH user configured on the remote authentication server must have the same username as the SSH user.

For an SFTP or SCP user, the working directory depends on the authentication method.

- If the authentication method is **publickey** or **password-publickey**, the working directory is specified by the **authorization-attribute** command in the associated local user view.
- If the authentication method is **keyboard-interactive** or **password**, the working directory is authorized by AAA.

For an SSH user, the user role also depends on the authentication method.

- If the authentication method is **publickey** or **password-publickey**, the user role is specified by the **authorization-attribute** command in the associated local user view.
- If the authentication method is **keyboard-interactive** or **password**, the user role is authorized by AAA.

If you use this command to specify a host public key or a PKI domain for a user multiple times, the most recent configuration takes effect. If neither a host public key nor a PKI domain is specified for the user, the user uses certificate authentication for login. The server uses the PKI domain of its own certificate to verify the client's certificate.

The command configuration does not affect logged-in users. It affects only users that attempt to log in after the configuration.

Examples

Create an SSH user named **user1**. Specify the service type as **sftp** and the authentication method as **password-publickey** for the user. Assign the host public key **key1** to the user.

```
<Sysname> system-view
[Sysname] ssh user user1 service-type sftp authentication-type password-publickey assign
publickey key1
```

Create a local device management user named **user1**. Specify the password as **123456TESTplat&!** in plain text and the service type as **ssh** for the user. Assign the working directory **flash:** and the **network-admin** user role to the user.

```
[Sysname] local-user user1 class manage
[Sysname-luser-manage-user1] password simple 123456TESTplat&!
[Sysname-luser-manage-user1] service-type ssh
[Sysname-luser-manage-user1] authorization-attribute work-directory flash: user-role
network-admin
```

Related commands

authorization-attribute

display ssh user-information

local-user

pki domain

SSH client commands

bye

Use **bye** to terminate the connection with the SFTP server and return to user view.

Syntax

bye

Views

SFTP client view

Predefined user roles

network-admin

network-operator

Usage guidelines

This command has the same function as the **exit** and **quit** commands.

Examples

Terminate the connection with the SFTP server.

```
sftp> bye
<Sysname>
```

cd

Use **cd** to change the working directory on the SFTP server.

Syntax

cd [*remote-path*]

Views

SFTP client view

Predefined user roles

network-admin

Parameters

remote-path: Specifies the name of a directory on the server.

Usage guidelines

You can use the **cd ..** command to return to the upper-level directory.

You can use the **cd /** command to return to the root directory of the system.

Examples

Change the working directory to **new1**.

```
sftp> cd new1
Current Directory is:/new1
sftp> pwd
Remote working directory: /new1
sftp>
```

cdup

Use **cdup** to return to the upper-level directory.

Syntax

cdup

Views

SFTP client view

Predefined user roles

network-admin

Example

Return to the upper-level directory from the current working directory **/test1**.

```
sftp> cd test1
Current Directory is:/test1
sftp> pwd
Remote working directory: /test1
sftp> cdup
Current Directory is:/
sftp> pwd
Remote working directory: /
sftp>
```

delete

Use **delete** to delete a file from the SFTP server.

Syntax

delete *remote-file*

Views

SFTP client view

Predefined user roles

network-admin

Parameters

remote-file: Specifies a file by its name.

Usage guidelines

This command has the same function as the **remove** command.

Examples

Delete file **temp.c** from the SFTP server.

```
sftp> delete temp.c
Removing /temp.c
```

delete ssh client server-public-key

Use **delete ssh client server-public-key** to delete server public key information saved in the public key file of the SSH client.

Syntax

delete ssh client server-public-key [**server-ip** *ip-address*]

Views

System view

Predefined user roles

network-admin

Parameters

server-ip *ip-address*: Specifies the IP address of the server whose public key information will be deleted. If you do not specify a server IP address, this command deletes the public keys of all servers from the client's public key file.

Examples

Delete all server public keys saved in the public key file of the SSH client.

```
<Sysname> system-view
[Sysname] delete ssh client server-public-key
Public keys of all SSH servers will be deleted. Continue? [Y/N]:y
```

Delete the public key of server 2.2.2.1 saved in the public key file of the SSH client.

```
<Sysname> system-view
[Sysname] delete ssh client server-public-key server-ip 2.2.2.1
```

dir

Use **dir** to display information about the files and subdirectories under a directory.

Syntax

dir [**-a** | **-l**] [*remote-path*]

Views

SFTP client view

Predefined user roles

network-admin

Parameters

-a: Displays detailed information about files and subdirectories under a directory in a list, including the files and subdirectories with names starting with dots (.).

-l: Displays detailed information about the files and subdirectories under a directory in a list, excluding the files and subdirectories with names starting with dots (.).

remote-path: Specifies the name of the directory to be queried. If you do not specify this argument, the command displays information about the files and subdirectories under the current working directory.

Usage guidelines

If you do not specify both of the **-a** and **-l** keywords, this command displays the names of the files and subdirectories under a directory.

This command has the same function as the **ls** command.

Examples

Display detailed information about the files and subdirectories under the current directory, including the files and subdirectories with names starting with dots (.).

```
sftp> dir -a
drwxrwxrwx    2 1        1               512 Dec 18 14:12 .
drwxrwxrwx    2 1        1               512 Dec 18 14:12 ..
-rwxrwxrwx    1 1        1               301 Dec 18 14:11 010.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 011.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 012.pub
```

Display detailed information about the files and subdirectories under the current directory, excluding the files and subdirectories with names starting with dots (.).

```
sftp> dir -l
-rwxrwxrwx    1 1        1               301 Dec 18 14:11 010.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 011.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 012.pub
```

display scp client source

Use **display scp client source** to display the source IP address configuration of the SCP client.

Syntax

display scp client source

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the source IP address configuration of the SCP client.

```
<Sysname> display scp client source
The source IP address of the SCP client is 192.168.0.1.
The source IPv6 address of the SCP client is 2:2::2:2.
```

Related commands

scp client ipv6 source
scp client source

display sftp client source

Use **display sftp client source** to display the source IP address configuration of the SFTP client.

Syntax

display sftp client source

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the source IP address configuration of the SFTP client.

```
<Sysname> display sftp client source
The source IP address of the SFTP client is 192.168.0.1
The source IPv6 address of the SFTP client is 2:2::2:2.
```

Related commands

sftp client ipv6 source

sftp client source

display ssh client server-public-key

Use **display ssh client server-public-key** to display server public key information saved in the public key file of the SSH client.

Syntax

display ssh client server-public-key [**server-ip** *ip-address*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

server-ip *ip-address*: Specifies the IP address of the server whose public key information will be displayed. If you do not specify a server IP address, this command displays the public keys of all servers saved in the client's public key file.

Usage guidelines

When a user connects to an unauthenticated server and selects to save the server's public key, the server public key will be saved to the public key file. Server public key information saved in the public

key file is not available in the configuration file. To display such server public key information on the SSH client, you must use this command.

Examples

Display all server public keys saved in the public key file of the SSH client.

```
<Sysname> display ssh client server-public-key
 Server address: 10.153.124.209
 Key type: ecdsa-sha2-nistp256
 Key length: 256
 Key code:
   AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAOGpJfwJExK
   eYb53KKqmrZ0V/XnYZKZEchyN9ax1IBt+toIXHeW5NfBE5ymeklPSNgQNhcndkU/
   422fT15UmgM=

 Server address: 2.2.2.1
 Key type: rsa
 Key length: 1024
 Key code:
   AAAAB3NzaC1yc2EAAAADAQABAAAAgQDIUrHbeLx/W7xElB1Ny3zeA8/uV9K6sj1p
   dSlhx5XcOatdNMoD/sioYgSsy9IxKZPqBs+vadqx/wCCB5+T2GLLu2qgaT0P9J+v
   RR/9Y8fI2b4tS7PoNf/QKDVD7XnoiZ+dqd0tnnRf6GV+74cp8ZEUQdAoTeDzzaAh
   7t6FbxrNrQ==
```

Display the public key of server 2.2.2.1 saved in the public key file of the SSH client.

```
<Sysname> display ssh client server-public-key server-ip 2.2.2.1
 Server address: 2.2.2.1
 Key type: rsa
 Key length: 1024
 Key code:
   AAAAB3NzaC1yc2EAAAADAQABAAAAgQDIUrHbeLx/W7xElB1Ny3zeA8/uV9K6sj1p
   dSlhx5XcOatdNMoD/sioYgSsy9IxKZPqBs+vadqx/wCCB5+T2GLLu2qgaT0P9J+v
   RR/9Y8fI2b4tS7PoNf/QKDVD7XnoiZ+dqd0tnnRf6GV+74cp8ZEUQdAoTeDzzaAh
   7t6FbxrNrQ==
```

Table 4 Command output

Field	Description
Server address	IP address of the SSH server.
Key type	Type of the public key: • **dsa**—DSA public key. • **ecdsa-sha2-nistp256**—256-bit ECDSA public key created by using the secp256r1 curve. • **ecdsa-sha2-nistp384**—384-bit ECDSA public key created by using the secp384r1 curve. • **rsa**—RSA public key.
Key length	Length of the public key, in bits.
Key code	Content of the public key.

display ssh client source

Use **display ssh client source** to display the source IP address configuration of the Stelnet client.

Syntax

display ssh client source

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the source IP address configuration of the Stelnet client.

```
<Sysname> display ssh client source
The source IP address of the SSH client is 192.168.0.1
The source IPv6 address of the SSH client is 2:2::2:2.
```

Related commands

ssh client ipv6 source

ssh client source

exit

Use **exit** to terminate the SFTP connection and return to user view.

Syntax

exit

Views

SFTP client view

Predefined user roles

network-admin

network-operator

Usage guidelines

This command has the same function as the **bye** and **quit** commands.

Examples

Terminate the SFTP connection.

```
sftp> exit
<Sysname>
```

get

Use **get** to download a file from the SFTP server and save it locally.

Syntax

get *remote-file* [*local-file*]

Views

SFTP client view

Predefined user roles

network-admin

Parameters

remote-file: Specifies the name of a file on the SFTP server.

local-file: Specifies the name for the local file. If you do not specify this argument, the file will be saved locally with the same name as the file on the SFTP server.

Examples

Download file **temp1.c** and save it as **temp.c** locally.

```
sftp> get temp1.c temp.c
Fetching /temp1.c to temp.c
/temp.c                                                100% 1424     1.4KB/s   00:00
```

help

Use **help** to display help information on the SFTP client.

Syntax

help

Views

SFTP client view

Predefined user roles

network-admin

network-operator

Usage guidelines

This command has the same function as entering the question mark (?).

Examples

Display help information on the SFTP client.

```
sftp> help
Available commands:
  bye                          Quit sftp
  cd [path]                    Change remote directory to 'path'
  cdup                         Change remote directory to the parent directory
  delete path                  Delete remote file
  dir [-a|-l][path]            Display remote directory listing
       -a                        List all filenames
       -l                        List filename including the specific
                                 information of the file
  exit                         Quit sftp
  get remote-path [local-path] Download file
  help                         Display this help text
```

```
ls [-a|-l][path]             Display remote directory
     -a                         List all filenames
     -l                         List filename including the specific
                                information of the file
mkdir path                   Create remote directory
put local-path [remote-path] Upload file
pwd                          Display remote working directory
quit                         Quit sftp
rename oldpath newpath       Rename remote file
remove path                  Delete remote file
rmdir path                   Delete remote empty directory
?                            Synonym for help
```

ls

Use **ls** to display information about the files and subdirectories under a directory.

Syntax

ls [**-a** | **-l**] [*remote-path*]

Views

SFTP client view

Predefined user roles

network-admin

Parameters

-a: Displays detailed information about files and subdirectories under a directory in a list, including the files and subdirectories with names starting with dots (.).

-l: Displays detailed information about the files and subdirectories under a directory in a list, excluding the files and subdirectories with names starting with dots (.).

remote-path: Specifies the name of the directory to be queried. If you do not specify this argument, the command displays information about the files and subdirectories under the current working directory.

Usage guidelines

If you do not specify both of the **-a** and **-l** keywords, this command displays the names of the files and subdirectories under a directory.

This command has the same function as the **dir** command.

Examples

Display detailed information about the files and subdirectories under the current directory, including the files and subdirectories with names starting with dots (.).

```
sftp> ls -a
drwxrwxrwx    2 1        1               512 Dec 18 14:12 .
drwxrwxrwx    2 1        1               512 Dec 18 14:12 ..
-rwxrwxrwx    1 1        1               301 Dec 18 14:11 010.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 011.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 012.pub
```

Display detailed information about the files and subdirectories under the current working directory, excluding the files and subdirectories with names starting with dots (.).

```
sftp> ls -l
-rwxrwxrwx    1 1        1               301 Dec 18 14:11 010.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 011.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 012.pub
```

mkdir

Use **mkdir** to create a directory on the SFTP server.

Syntax

mkdir *remote-path*

Views

SFTP client view

Predefined user roles

network-admin

Parameters

remote-path: Specifies the name of a directory.

Examples

Create a directory named **test** on the SFTP server.

```
sftp> mkdir test
```

put

Use **put** to upload a local file to the SFTP server.

Syntax

put *local-file* [*remote-file*]

Views

SFTP client view

Predefined user roles

network-admin

Parameters

local-file: Specifies the name of a local file.

remote-file: Specifies the name of a file on an SFTP server. If you do not specify this argument, the file will be remotely saved with the same name as the local file.

Examples

Upload the local file **startup.bak** to the SFTP server and save it as **startup01.bak**.

```
sftp> put startup.bak startup01.bak
Uploading startup.bak to /startup01.bak
startup01.bak                                 100% 1424     1.4KB/s   00:00
```

pwd

Use **pwd** to display the current working directory of the SFTP server.

Syntax

pwd

Views

SFTP client view

Predefined user roles

network-admin

Examples

Display the current working directory of the SFTP server.

```
sftp> pwd
Remote working directory: /
```

The output shows that the current working directory is the root directory.

quit

Use **quit** to terminate the SFTP connection and return to user view.

Syntax

quit

Views

SFTP client view

Predefined user roles

network-admin

network-operator

Usage guidelines

This command has the same function as the **bye** and **exit** commands.

Examples

Terminate the SFTP connection.

```
sftp> quit
<Sysname>
```

remove

Use **remove** to delete a file from the SFTP server.

Syntax

remove *remote-file*

Views

SFTP client view

Predefined user roles

network-admin

Parameters

remote-file: Specifies a file by its name.

Usage guidelines

This command has the same function as the **delete** command.

Examples

Delete file **temp.c** from the SFTP server.

```
sftp> remove temp.c
Removing /temp.c
```

rename

Use **rename** to change the name of a file or directory on the SFTP server.

Syntax

rename *old-name new-name*

Views

SFTP client view

Predefined user roles

network-admin

Parameters

oldname: Specifies the name of an existing file or directory.

newname: Specifies a new name for the existing file or directory.

Examples

Change the name of a file on the SFTP server from **temp1.c** to **temp2.c**.

```
sftp> dir
aa.pub  temp1.c
sftp> rename temp1.c temp2.c
sftp> dir
aa.pub  temp2.c
```

rmdir

Use **rmdir** to delete a directory from the SFTP server.

Syntax

rmdir *remote-path*

Views

SFTP client view

Predefined user roles

network-admin

Parameters

remote-path: Specifies a directory.

Examples

Delete subdirectory **temp1** under the current directory on the SFTP server.

```
sftp> rmdir temp1
```

scp

Use **scp** to establish a connection to an IPv4 SCP server and transfer files with the server.

Syntax

In non-FIPS mode:

scp *server* [*port-number*] { **put** | **get** } *source-file-name* [*destination-file-name*] [**identity-key** { **dsa** | **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | { **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } **pki-domain** *domain-name* } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [{ **public-key** *keyname* | **server-pki-domain** *domain-name* } | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] * [**user** *username* [**password** *password*]]

In FIPS mode:

scp *server* [*port-number*] { **put** | **get** } *source-file-name* [*destination-file-name*] [**identity-key** { **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | { **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } **pki-domain** *domain-name* } | **prefer-compress zlib** | **prefer-ctos-cipher** { **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** } | **prefer-ctos-hmac** { **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** } | **prefer-stoc-hmac** { **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [{ **public-key** *keyname* | **server-pki-domain** *domain-name* } | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] * [**user** *username* [**password** *password*]]

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv4 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range of 1 to 65535. The default is 22.

get: Downloads the file.

put: Uploads the file.

source-file-name: Specifies the name of the source file, a case-sensitive string of 1 to 255 characters.

destination-file-name: Specifies the name of the target file, a case-sensitive string of 1 to 255 characters. If you do not specify this argument, the target file uses the same file name as the source file.

identity-key: Specifies a public key algorithm for publickey authentication of the client. The default is DSA in non-FIPS mode and is RSA in FIPS mode. If the server uses publickey authentication, you must specify this keyword. The client generates the digital signature or certificate by using the local private key that is associated with the specified algorithm.

- **dsa**: Specifies public key algorithm DSA.
- **ecdsa-sha2-nistp256**: Specifies public key algorithm ecdsa-sha2-nistp256.
- **ecdsa-sha2-nistp384**: Specifies public key algorithm ecdsa-sha2-nistp384.
- **rsa**: Specifies public key algorithm RSA.
- **x509v3-ecdsa-sha2-nistp256**: Specifies public key algorithm x509v3-ecdsa-sha2-nistp256.
- **x509v3-ecdsa-sha2-nistp384**: Specifies public key algorithm x509v3-ecdsa-sha2-nistp384.
- **pki-domain** *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument is a case-insensitive string of 1 to 31 characters. When the x509v3 public key algorithm is used, you must specify this option for the client to get the correct local certificate.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies compression algorithm zlib.

prefer-ctos-cipher: Specifies the preferred client-to-server encryption algorithm. The default is AES128-CTR. Supported algorithms are DES-CBC, 3DES-CBC, AES128-CBC, AES128-CTR, AES128-GCM, AES192-CTR, AES256-CBC, AES256-CTR, and AES256-GCM in ascending order of security strength and computation time.

- **3des-cbc**: Specifies encryption algorithm 3DES-CBC.
- **aes128-cbc**: Specifies encryption algorithm AES128-CBC.
- **aes128-ctr**: Specifies encryption algorithm AES128-CTR.
- **aes128-gcm**: Specifies encryption algorithm AES128-GCM.
- **aes192-ctr**: Specifies encryption algorithm AES192-CTR.
- **aes256-cbc**: Specifies encryption algorithm AES256-CBC.
- **aes256-ctr**: Specifies encryption algorithm AES256-CTR.
- **aes256-gcm**: Specifies encryption algorithm AES256-GCM.
- **des-cbc**: Specifies encryption algorithm DES-CBC.

prefer-ctos-hmac: Specifies the preferred client-to-server HMAC algorithm. The default is SHA2-256.Supported algorithms are MD5, MD5-96, SHA1, SHA1-96, SHA2-256, and SHA2-512 in ascending order of security strength and computation time.

- **md5**: Specifies HMAC algorithm HMAC-MD5.
- **md5-96**: Specifies HMAC algorithm HMAC-MD5-96.
- **sha1**: Specifies HMAC algorithm HMAC-SHA1.
- **sha1-96**: Specifies HMAC algorithm HMAC-SHA1-96.
- **sha2-256**: Specifies HMAC algorithm HMAC-SHA2-256.
- **sha2-512**: Specifies HMAC algorithm HMAC-SHA2-512.

prefer-kex: Specifies the preferred key exchange algorithm. The default is ecdh-sha2-nistp256. Supported algorithms are diffie-hellman-group-exchange-sha1, diffie-hellman-group1-sha1, diffie-hellman-group14-sha1, ecdh-sha2-nistp256, and ecdh-sha2-nistp384, in ascending order of security strength and computation time.

- **dh-group-exchange-sha1**: Specifies key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1-sha1**: Specifies key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14-sha1**: Specifies key exchange algorithm diffie-hellman-group14-sha1.
- **ecdh-sha2-nistp256**: Specifies key exchange algorithm ecdh-sha2-nistp256.
- **ecdh-sha2-nistp384**: Specifies key exchange algorithm ecdh-sha2-nistp384.

prefer-stoc-cipher: Specifies the preferred server-to-client encryption algorithm. The default is AES128-CTR. Supported algorithms are the same as the client-to-server encryption algorithms (see the **prefer-ctos-cipher** keyword).

prefer-stoc-hmac: Specifies the preferred server-to-client HMAC algorithm. The default is SHA2-256. Supported algorithms are the same as the client-to-server HMAC algorithms (see the **prefer-ctos-hmac** keyword).

public-key *keyname*: Specifies the server's host public key that the client uses to authenticate the server. The *keyname* argument is a case-insensitive string of 1 to 64 characters.

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

source: Specifies a source IPv4 address or source interface for SCP packets. By default, the device uses the primary IPv4 address of the output interface in the routing entry as the source address of SCP packets. As a best practice to ensure successful SCP connections, specify a loopback interface as the source interface or specify the IPv4 address of a loopback interface as the source address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The IPv4 address of this interface is the source IPv4 address of the SCP packets.
- **ip** *ip-address*: Specifies a source IPv4 address.

user *username*: Specifies an SCP username, a case-sensitive string of 1 to 80 characters. If the username contains an ISP domain name, use the *pureusername@domain*, *pureusername*/*domain*, or *domain**pureusername* format.

password *password*: Specifies a password in plaintext form, a case-sensitive string of 1 to 63 characters.

Usage guidelines

If the client and the server have negotiated to use certificate authentication, the client must verify the server's certificate. For the client to correctly get the server's certificate, you must specify the server's PKI domain on the client by using the **server-pki-domain** *domain-name* option. The client uses the CA certificate stored in the specified PKI domain to verify the server's certificate and does not need to save the server's public key before authentication. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

If you do not specify a username and password in the command, you must provide the username and password in an interactive way.

If the SCP server uses publickey authentication, the password specified by this command is ignored.

Examples

Connect the SCP client to SCP server **200.1.1.1**. Specify the public key of the server as **svkey**, and download file **abc.txt** from the server. The SCP client uses publickey authentication. Use the following algorithms:

- Preferred key exchange algorithm: **dh-group14-sha1**.

- Preferred server-to-client encryption algorithm: **aes128-cbc**.
- Preferred client-to-server HMAC algorithm: **sha1**.
- Preferred server-to-client HMAC algorithm: **sha1-96**.
- Preferred compression algorithm: **zlib**.

```
<Sysname> scp 200.1.1.1 get abc.txt prefer-kex dh-group14-sha1 prefer-stoc-cipher
aes128-cbc prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key
svkey
Username:
```

scp client ipv6 source

Use **scp client ipv6 source** to configure the source IPv6 address for SCP packets that are sent by the SCP client.

Use **undo scp client ipv6 source** to restore the default.

Syntax

scp client ipv6 source { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }

undo scp client ipv6 source

Default

The source IPv6 address for outgoing SCP packets is not configured. The SCP client automatically selects an IPv6 address for outgoing SCP packets in compliance with RFC 3484.

Views

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a source interface by its type and number. The SCP client selects the interface's address that most specifically matches the destination address of outgoing SCP packets as the source address of the SCP packets.

ipv6 *ipv6-address*: Specifies a source IPv6 address.

Usage guidelines

This command takes effect on all IPv6 SCP connections. The source IPv6 address specified in the **scp ipv6** command takes effect only on the current IPv6 SCP connection. If you specify the source IPv6 address in both this command and the **scp ipv6** command, the source IPv6 address specified in the **scp ipv6** command takes effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify **2:2::2:2** as the source IPv6 address for SCP packets.

```
<Sysname> system-view
[Sysname] scp client ipv6 source ipv6 2:2::2:2
```

Related commands

display scp client source

scp client source

Use **scp client source** to configure the source IPv4 address for SCP packets that are sent by the SCP client.

Use **undo scp client source** to restore the default.

Syntax

scp client source { **interface** *interface-type interface-number* | **ip** *ip-address* }

undo scp client source

Default

The source IPv4 address for outgoing SCP packets is not configured. The SCP client uses the primary IPv4 address of the output interface in the matching route as the source IPv4 address for outgoing SCP packets.

Views

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a source interface by its type and number. The SCP client uses the primary IPv4 address of the interface as the source address of outgoing SCP packets.

ip *ip-address*: Specifies a source IPv4 address.

Usage guidelines

This command takes effect on all SCP connections. The source IPv4 address specified in the **scp** command takes effect only on the current SCP connection. If you specify the source IPv4 address in both this command and the **scp** command, the source IPv4 address specified in the **scp** command takes effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify **192.168.0.1** as the source IPv4 address for SCP packets.

```
<Sysname> system-view
[Sysname] scp client source ip 192.168.0.1
```

Related commands

display scp client source

scp ipv6

Use **scp ipv6** to establish a connection to an IPv6 SCP server and transfer files with the server.

Syntax

In non-FIPS mode:

scp ipv6 *server* [*port-number*] [**-i** *interface-type interface-number*] { **put** | **get** } *source-file-name* [*destination-file-name*] [**identity-key** { **dsa** | **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** |

{ **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } **pki-domain** *domain-name* } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [{ **public-key** *keyname* | **server-pki-domain** *domain-name* } | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] * [**user** *username* [**password** *password*]]

In FIPS mode:

scp ipv6 *server* [*port-number*] [**-i** *interface-type interface-number*] { **put** | **get** } *source-file-name* [*destination-file-name*] [**identity-key** { **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | { **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } **pki-domain** *domain-name* } | **prefer-compress zlib** | **prefer-ctos-cipher** { **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** } | **prefer-ctos-hmac** { **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** } | **prefer-stoc-hmac** { **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [{ **public-key** *keyname* | **server-pki-domain** *domain-name* } | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] * [**user** *username* [**password** *password*]]

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv6 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range of 1 to 65535. The default is 22.

-i *interface-type interface-number:* Specifies an output interface by its type and number for SCP packets. This option is used only when the server uses a link-local address to provide the SCP service for the client. The specified output interface on the SCP client must have a link-local address.

get: Downloads the file.

put: Uploads the file.

source-file-name: Specifies the name of the source file, a case-sensitive string of 1 to 255 characters.

destination-file-name: Specifies the name of the target file, a case-sensitive string of 1 to 255 characters. If you do not specify this argument, the target file uses the same file name as the source file.

identity-key: Specifies a public key algorithm for publickey authentication of the client. The default is DSA in non-FIPS mode and is RSA in FIPS mode. If the server uses publickey authentication, you must specify this keyword. The client generates the digital signature or certificate by using the local private key that is associated with the specified algorithm.

- **dsa**: Specifies public key algorithm DSA.
- **ecdsa-sha2-nistp256**: Specifies public key algorithm ecdsa-sha2-nistp256.
- **ecdsa-sha2-nistp384**: Specifies public key algorithm ecdsa-sha2-nistp384.
- **rsa**: Specifies public key algorithm RSA.
- **x509v3-ecdsa-sha2-nistp256**: Specifies public key algorithm x509v3-ecdsa-sha2-nistp256.

  x509v3-ecdsa-sha2-nistp384: Specifies public key algorithm x509v3-ecdsa-sha2-nistp384.
- **pki-domain** *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument is a case-insensitive string of 1 to 31 characters. When the x509v3 public key algorithm is used, you must specify this option for the client to get the correct local certificate.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies compression algorithm zlib.

prefer-ctos-cipher: Specifies the preferred client-to-server encryption algorithm. The default is AES128-CTR. Supported algorithms are DES-CBC, 3DES-CBC, AES128-CBC, AES128-CTR, AES128-GCM, AES192-CTR, AES256-CBC, AES256-CTR, and AES256-GCM in ascending order of security strength and computation time.

- **3des-cbc**: Specifies encryption algorithm 3DES-CBC.
- **aes128-cbc**: Specifies encryption algorithm AES128-CBC.
- **aes128-ctr**: Specifies encryption algorithm AES128-CTR.
- **aes128-gcm**: Specifies encryption algorithm AES128-GCM.
- **aes192-ctr**: Specifies encryption algorithm AES192-CTR.
- **aes256-cbc**: Specifies encryption algorithm AES256-CBC.
- **aes256-ctr**: Specifies encryption algorithm AES256-CTR.
- **aes256-gcm**: Specifies encryption algorithm AES256-GCM.
- **des-cbc**: Specifies encryption algorithm DES-CBC.

prefer-ctos-hmac: Specifies the preferred client-to-server HMAC algorithm. The default is SHA2-256. Supported algorithms are MD5, MD5-96, SHA1, SHA1-96, SHA2-256, and SHA2-512 in ascending order of security strength and computation time.

- **md5**: Specifies HMAC algorithm HMAC-MD5.
- **md5-96**: Specifies HMAC algorithm HMAC-MD5-96.
- **sha1**: Specifies HMAC algorithm HMAC-SHA1.
- **sha1-96**: Specifies HMAC algorithm HMAC-SHA1-96.
- **sha2-256**: Specifies HMAC algorithm HMAC-SHA2-256.
- **sha2-512**: Specifies HMAC algorithm HMAC-SHA2-512.

prefer-kex: Specifies the preferred key exchange algorithm. The default is ecdh-sha2-nistp256. Supported algorithms are diffie-hellman-group-exchange-sha1, diffie-hellman-group1-sha1, diffie-hellman-group14-sha1, ecdh-sha2-nistp256, and ecdh-sha2-nistp384, in ascending order of security strength and computation time.

- **dh-group-exchange-sha1**: Specifies key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1-sha1**: Specifies key exchange algorithm diffie-hellman-group1-sha1.

- **dh-group14-sha1**: Specifies key exchange algorithm diffie-hellman-group14-sha1.
- **ecdh-sha2-nistp256**: Specifies key exchange algorithm ecdh-sha2-nistp256.
- **ecdh-sha2-nistp384**: Specifies key exchange algorithm ecdh-sha2-nistp384.

prefer-stoc-cipher: Specifies the preferred server-to-client encryption algorithm. The default is AES128-CTR. Supported algorithms are the same as the client-to-server encryption algorithms (see the **prefer-ctos-cipher** keyword).

prefer-stoc-hmac: Specifies the preferred server-to-client HMAC algorithm. The default is SHA2-256. Supported algorithms are the same as the client-to-server HMAC algorithms (see the **prefer-ctos-hmac** keyword).

public-key *keyname*: Specifies the server's host public key that the client uses to authenticate the server. The *keyname* argument is a case-insensitive string of 1 to 64 characters.

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

source: Specifies a source IPv6 address or source interface for IPv6 SCP packets. By default, the device automatically selects a source address for IPv6 SCP packets in compliance with RFC 3484. As a best practice to ensure successful SCP connections, specify a loopback interface as the source interface or specify the IPv6 address of a loopback interface as the source address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The IPv6 address of this interface is the source IPv6 address of the IPv6 SCP packets.
- **ipv6** *ipv6-address*: Specifies a source IPv6 address.

user *username*: Specifies an SCP username, a case-sensitive string of 1 to 80 characters. If the username contains an ISP domain name, use the *pureusername@domain*, *pureusername*/*domain*, or *domain**pureusername* format.

password *password*: Specifies a password in plaintext form, a case-sensitive string of 1 to 63 characters.

Usage guidelines

If the client and the server have negotiated to use certificate authentication, the client must verify the server's certificate. For the client to correctly get the server's certificate, you must specify the server's PKI domain on the client by using the **server-pki-domain** *domain-name* option. The client uses the CA certificate stored in the specified PKI domain to verify the server's certificate and does not need to save the server's public key before authentication. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

If you do not specify a username and password in the command, you must provide the username and password in an interactive way.

If the SCP server uses publickey authentication, the password specified by this command is ignored.

Examples

Connect an SCP client to SCP server **2000::1**. Specify the public key of the server as **svkey**, and download file **abc.txt** from the server. The SCP client uses publickey authentication. Use the following algorithms:

- Preferred key exchange algorithm: **dh-group14-sha1**.
- Preferred server-to-client encryption algorithm: **aes128-cbc**.
- Preferred client-to-server HMAC algorithm: **sha1**.
- Preferred server-to-client HMAC algorithm: **sha1-96**.
- Preferred compression algorithm: **zlib**.

```
<Sysname> scp ipv6 2000::1 get abc.txt prefer-kex dh-group14-sha1 prefer-stoc-cipher
aes128-cbc prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key
svkey
Username:
```

scp ipv6 suite-b

Use **scp ipv6 suite-b** to establish a connection to an IPv6 SCP server based on Suite B algorithms and transfer files with the server.

Syntax

scp ipv6 *server* [*port-number*] [**-i** *interface-type interface-number*] { **put** | **get** } *source-file-name* [*destination-file-name*] **suite-b** [**128-bit** | **192-bit**] **pki-domain** *domain-name* [**server-pki-domain** *domain-name*] [**prefer-compress zlib**] [**source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] * [**user** *username* [**password** *password*]]

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv6 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range of 1 to 65535. The default is 22.

-i *interface-type interface-number:* Specifies an output interface by its type and number for SCP packets. Specify this option when the server uses a link-local address to provide the SCP service for the client. The specified output interface on the SCP client must have a link-local address.

get: Downloads the file.

put: Uploads the file.

source-file-name: Specifies the name of the source file, a case-sensitive string of 1 to 255 characters.

destination-file-name: Specifies the name of the target file, a case-sensitive string of 1 to 255 characters. If you do not specify this argument, the target file uses the same file name as the source file.

suite-b: Specifies the Suite B algorithms. If neither the 128-bit keyword nor the 192-bit keyword is specified, all algorithms in Suite B are used. For more information about the Suite B algorithms, see Table 5.

128-bit: Specifies the 128-bit Suite B security level.

192-bit: Specifies the 192-bit Suite B security level.

pki-domain *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string

of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes ('). If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies compression algorithm zlib.

source: Specifies a source IPv6 address or source interface for IPv6 SCP packets. By default, the device automatically selects a source address for IPv6 SCP packets in compliance with RFC 3484. As a best practice to ensure successful SCP connections, specify a loopback interface as the source interface or specify the IPv6 address of a loopback interface as the source address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The IPv6 address of this interface is the source IPv6 address of the IPv6 SCP packets.
- **ipv6** *ipv6-address*: Specifies a source IPv6 address.

user *username*: Specifies an SCP username, a case-sensitive string of 1 to 80 characters. If the username contains an ISP domain name, use the *pureusername@domain*, *pureusername*/*domain*, or *domain**pureusername* format.

password *password*: Specifies a password in plaintext form, a case-sensitive string of 1 to 63 characters.

Usage guidelines

Table 5 Suite B algorithms

Security level	Key exchange algorithm	Encryption algorithm and HMAC algorithm	Public key algorithm
128-bit	ecdh-sha2-nistp256	AES128-GCM	x509v3-ecdsa-sha2-nistp256
192-bit	ecdh-sha2-nistp384	AES256-GCM	x509v3-ecdsa-sha2-nistp384
Both	ecdh-sha2-nistp256 ecdh-sha2-nistp384	AES128-GCM AES256-GCM	x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384

If you do not specify a username and password in the command, you must provide the username and password in an interactive way.

If the SCP server uses publickey authentication, the password specified by this command is ignored.

Examples

Use the 192-bit Suite B algorithms to establish a connection to SCP server **2000::1** and download the file **abc.txt** from the server. Specify the client's PKI domain and the server's PKI domain as **clientpkidomain** and **serverpkidomain**, respectively.

```
<Sysname> scp ipv6 2000::1 get abc.txt suite-b 192-bit pki-domain clientpkidomain
server-pki-domain serverpkidomain
Username:
```

scp suite-b

Use **scp suite-b** to establish a connection to an SCP server based on Suite B algorithms and transfer files with the server.

Syntax

scp *server* [*port-number*] { **put** | **get** } *source-file-name* [*destination-file-name*] **suite-b** [**128-bit** | **192-bit**] **pki-domain** *domain-name* [**server-pki-domain** *domain-name*] [**prefer-compress zlib**] [**source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] * [**user** *username* [**password** *password*]]

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv4 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range of 1 to 65535. The default is 22.

get: Downloads the file.

put: Uploads the file.

source-file-name: Specifies the name of the source file, a case-sensitive string of 1 to 255 characters.

destination-file-name: Specifies the name of the target file, a case-sensitive string of 1 to 255 characters. If you do not specify this argument, the target file uses the same file name as the source file.

suite-b: Specifies the Suite B algorithms. If neither the 128-bit keyword nor the 192-bit keyword is specified, all algorithms in Suite B are used. For more information about the Suite B algorithms, see Table 6.

128-bit: Specifies the 128-bit Suite B security level.

192-bit: Specifies the 192-bit Suite B security level.

pki-domain *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes ('). If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies compression algorithm zlib.

source: Specifies a source IP address or source interface for SCP packets. By default, the device uses the primary IPv4 address of the output interface in the routing entry as the source address of SCP packets. As a best practice to ensure successful SCP connections, specify a loopback interface as the source interface or specify the IPv4 address of a loopback interface as the source address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The IPv4 address of this interface is the source IPv4 address of the SCP packets.

- **ip** *ip-address*: Specifies a source IPv4 address.

user *username*: Specifies an SCP username, a case-sensitive string of 1 to 80 characters. If the username contains an ISP domain name, use the *pureusername@domain*, *pureusername*/*domain*, or *domain**pureusername* format.

password *password*: Specifies a password in plaintext form, a case-sensitive string of 1 to 63 characters.

Usage guidelines

Table 6 Suite B algorithms

Security level	Key exchange algorithm	Encryption algorithm and HMAC algorithm	Public key algorithm
128-bit	ecdh-sha2-nistp256	AES128-GCM	x509v3-ecdsa-sha2-nistp256
192-bit	ecdh-sha2-nistp384	AES256-GCM	x509v3-ecdsa-sha2-nistp384
Both	ecdh-sha2-nistp256 ecdh-sha2-nistp384	AES128-GCM AES256-GCM	x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384

If you do not specify a username and password in the command, you must provide the username and password in an interactive way.

If the SCP server uses publickey authentication, the password specified by this command is ignored.

Examples

Use the 128-bit Suite B algorithms to establish a connection to SCP server **200.1.1.1** and download the file **abc.txt** from the server. Specify the client's PKI domain and the server's PKI domain as **clientpkidomain** and **serverpkidomain**, respectively.

```
<Sysname> scp 200.1.1.1 get abc.txt suite-b 128-bit pki-domain clientpkidomain
server-pki-domain serverpkidomain
Username
```

sftp

Use **sftp** to establish a connection to an IPv4 SFTP server and enter SFTP client view.

Syntax

In non-FIPS mode:

sftp *server* [*port-number*] [**identity-key** { **dsa** | **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | { **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } **pki-domain** *domain-name* } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [**dscp** *dscp-value* | { **public-key** *keyname* | **server-pki-domain** *domain-name* } | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *

In FIPS mode:

sftp *server* [*port-number*] [**identity-key** { **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | { **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } **pki-domain** *domain-name* } | **prefer-compress** **zlib** | **prefer-ctos-cipher** { **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** } | **prefer-ctos-hmac** { **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** } | **prefer-stoc-hmac** { **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [{ **public-key** *keyname* | **server-pki-domain** *domain-name* } | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv4 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range of 1 to 65535. The default is 22.

identity-key: Specifies a public key algorithm for publickey authentication of the client. The default is DSA in non-FIPS mode and is RSA in FIPS mode. If the server uses publickey authentication, you must specify this keyword. The client generates the digital signature or certificate by using the local private key that is associated with the specified algorithm.

- **dsa**: Specifies public key algorithm DSA.
- **ecdsa-sha2-nistp256**: Specifies public key algorithm ecdsa-sha2-nistp256.
- **ecdsa-sha2-nistp384**: Specifies public key algorithm ecdsa-sha2-nistp384.
- **rsa**: Specifies public key algorithm RSA.
- **x509v3-ecdsa-sha2-nistp256**: Specifies public key algorithm x509v3-ecdsa-sha2-nistp256.
- **x509v3-ecdsa-sha2-nistp384**: Specifies public key algorithm x509v3-ecdsa-sha2-nistp384.
- **pki-domain** *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument is a case-insensitive string of 1 to 31 characters. When the x509v3 public key algorithm is used, you must specify this option for the client to get the correct local certificate.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies compression algorithm zlib.

prefer-ctos-cipher: Specifies the preferred client-to-server encryption algorithm. The default is AES128-CTR. Supported algorithms are DES-CBC, 3DES-CBC, AES128-CBC, AES128-CTR, AES128-GCM, AES192-CTR, AES256-CBC, AES256-CTR, and AES256-GCM in ascending order of security strength and computation time.

- **3des-cbc**: Specifies encryption algorithm 3DES-CBC.
- **aes128-cbc**: Specifies encryption algorithm AES128-CBC.
- **aes128-ctr**: Specifies encryption algorithm AES128-CTR.
- **aes128-gcm**: Specifies encryption algorithm AES128-GCM.

- **aes192-ctr**: Specifies encryption algorithm AES192-CTR.
- **aes256-cbc**: Specifies encryption algorithm AES256-CBC.
- **aes256-ctr**: Specifies encryption algorithm AES256-CTR.
- **aes256-gcm**: Specifies encryption algorithm AES256-GCM.
- **des-cbc**: Specifies encryption algorithm DES-CBC.

prefer-ctos-hmac: Specifies the preferred client-to-server HMAC algorithm. The default is SHA2-256. Supported algorithms are MD5, MD5-96, SHA1, SHA1-96, SHA2-256, and SHA2-512 in ascending order of security strength and computation time.

- **md5**: Specifies HMAC algorithm HMAC-MD5.
- **md5-96**: Specifies HMAC algorithm HMAC-MD5-96.
- **sha1**: Specifies HMAC algorithm HMAC-SHA1.
- **sha1-96**: Specifies HMAC algorithm HMAC-SHA1-96.
- **sha2-256**: Specifies HMAC algorithm HMAC-SHA2-256.
- **sha2-512**: Specifies HMAC algorithm HMAC-SHA2-512.

prefer-kex: Specifies the preferred key exchange algorithm. The default is ecdh-sha2-nistp256. Supported algorithms are diffie-hellman-group-exchange-sha1, diffie-hellman-group1-sha1, diffie-hellman-group14-sha1, ecdh-sha2-nistp256, and ecdh-sha2-nistp384, in ascending order of security strength and computation time.

- **dh-group-exchange-sha1**: Specifies key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1-sha1**: Specifies key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14-sha1**: Specifies key exchange algorithm diffie-hellman-group14-sha1.
- **ecdh-sha2-nistp256**: Specifies key exchange algorithm ecdh-sha2-nistp256.
- **ecdh-sha2-nistp384**: Specifies key exchange algorithm ecdh-sha2-nistp384.

prefer-stoc-cipher: Specifies the preferred server-to-client encryption algorithm. The default is AES128-CTR. Supported algorithms are the same as the client-to-server encryption algorithms (see the **prefer-ctos-cipher** keyword).

prefer-stoc-hmac: Specifies the preferred server-to-client HMAC algorithm. The default is SHA2-256. Supported algorithms are the same as the client-to-server HMAC algorithms (see the **prefer-ctos-hmac** keyword).

dscp *dscp-value*: Specifies the DSCP value in the IPv4 SFTP packets. The value range for the *dscp-value* argument is 0 to 63, and the default value is 48. The DSCP value determines the transmission priority of the packet.

public-key *keyname*: Specifies the server's host public key that the client uses to authenticate the server. The *keyname* argument is a case-insensitive string of 1 to 64 characters.

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

source: Specifies a source IPv4 address or source interface for the SFTP packets. By default, the device uses the primary IPv4 address of the output interface in the routing entry as the source address of SFTP packets. As a best practice to ensure successful SFTP connections, specify a loopback interface as the source interface or specify the IPv4 address of a loopback interface as the source address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The primary IPv4 address of this interface is the source IPv4 address of the SFTP packets.
- **ip** *ip-address*: Specifies a source IPv4 address.

Usage guidelines

If the client and the server have negotiated to use certificate authentication, the client must verify the server's certificate. For the client to correctly get the server's certificate, you must specify the server's PKI domain on the client by using the **server-pki-domain** *domain-name* option. The client uses the CA certificate stored in the specified PKI domain to verify the server's certificate and does not need to save the server's public key before authentication. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

Examples

Connect an SFTP client to SFTP server **10.1.1.2** and specify the public key of the server as **svkey**. The SFTP client uses publickey authentication. Use the following algorithms:

- Preferred key exchange algorithm: **dh-group14-sha1**.
- Preferred server-to-client encryption algorithm: **aes128-cbc**.
- Preferred client-to-server HMAC algorithm: **sha1**.
- Preferred server-to-client HMAC algorithm: **sha1-96**.
- Preferred compression algorithm: **zlib**.

```
<Sysname> sftp 10.1.1.2 prefer-kex dh-group14-sha1 prefer-stoc-cipher aes128-cbc
prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key svkey
```

sftp client ipv6 source

Use **sftp client ipv6 source** to configure the source IPv6 address for SFTP packets that are sent by the SFTP client.

Use **undo sftp client ipv6 source** to restore the default.

Syntax

sftp client ipv6 source { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }

undo sftp client ipv6 source

Default

The source IPv6 address for outgoing SFTP packets is not configured. The SFTP client automatically selects an IPv6 address for outgoing SFTP packets in compliance with RFC 3484.

Views

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a source interface by its type and number. The SFTP client selects the interface's address that most specifically matches the destination address of outgoing SFTP packets as the source address of the SFTP packets.

ipv6 *ipv6-address*: Specifies a source IPv6 address.

Usage guidelines

This command takes effect on all IPv6 SFTP connections. The source IPv6 address specified in the **sftp ipv6** command takes effect only on the current IPv6 SFTP connection. If you specify the source IPv6 address both in this command and the **sftp ipv6** command, the source IPv6 address specified in the **sftp ipv6** command takes effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify **2:2::2:2** as the source IPv6 address for SFTP packets.

```
<Sysname> system-view
[Sysname] sftp client ipv6 source ipv6 2:2::2:2
```

Related commands

display sftp client source

sftp client source

Use **sftp client source** to configure the source IPv4 address for SFTP packets that are sent by the SFTP client.

Use **undo sftp client source** to restore the default.

Syntax

sftp client source { **interface** *interface-type interface-number* | **ip** *ip-address* }

undo sftp client source

Default

The source IPv4 address for outgoing SFTP packets is not configured. The SFTP client uses the primary IPv4 address of the output interface in the matching route as the source IPv4 address of outgoing SFTP packets.

Views

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a source interface by its type and number. The SFTP client uses the primary IPv4 address of the interface as the source address of outgoing SFTP packets.

ip *ip-address*: Specifies a source IPv4 address.

Usage guidelines

This command takes effect on all SFTP connections. The source IPv4 address specified in the **sftp** command takes effect only on the current SFTP connection. If you specify the source IPv4 address both in this command and the **sftp** command, the source IPv4 address specified in the **sftp** command takes effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify **192.168.0.1** as the source IPv4 address for SFTP packets.

```
<Sysname> system-view
[Sysname] sftp client source ip 192.168.0.1
```

Related commands

display sftp client source

sftp ipv6

Use **sftp ipv6** to connect an SFTP client to an IPv6 SFTP server and enter SFTP client view.

Syntax

In non-FIPS mode:

sftp ipv6 *server* [*port-number*] [**-i** *interface-type interface-number*] [**identity-key** { **dsa** | **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | { **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } **pki-domain** *domain-name* } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [**dscp** *dscp-value* | { **public-key** *keyname* | **server-pki-domain** *domain-name* } | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

In FIPS mode:

sftp ipv6 *server* [*port-number*] [**-i** *interface-type interface-number*] [**identity-key** { **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | { **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } **pki-domain** *domain-name* } | **prefer-compress zlib** | **prefer-ctos-cipher** { **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** } | **prefer-ctos-hmac** { **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** } | **prefer-stoc-hmac** { **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [{ **public-key** *keyname* | **server-pki-domain** *domain-name* } | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv6 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range of 1 to 65535. The default is 22.

-i *interface-type interface-number:* Specifies an output interface by its type and number for IPv6 SFTP packets. This option is used only when the server uses a link-local address to

provide the SFTP service for the client. The specified output interface on the SFTP client must have a link-local address.

identity-key: Specifies a public key algorithm for publickey authentication of the client. The default is DSA in non-FIPS mode and is RSA in FIPS mode. If the server uses publickey authentication, you must specify this keyword. The client generates the digital signature or certificate by using the local private key that is associated with the specified algorithm.

- **dsa**: Specifies public key algorithm DSA.
- **ecdsa-sha2-nistp256**: Specifies public key algorithm ecdsa-sha2-nistp256.
- **ecdsa-sha2-nistp384**: Specifies public key algorithm ecdsa-sha2-nistp384.
- **rsa**: Specifies public key algorithm RSA.
- **x509v3-ecdsa-sha2-nistp256**: Specifies public key algorithm x509v3-ecdsa-sha2-nistp256.
- **x509v3-ecdsa-sha2-nistp384**: Specifies public key algorithm x509v3-ecdsa-sha2-nistp384.
- **pki-domain** *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument is a case-insensitive string of 1 to 31 characters. When the x509v3 public key algorithm is used, you must specify this option for the client to get the correct local certificate.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies compression algorithm zlib.

prefer-ctos-cipher: Specifies the preferred client-to-server encryption algorithm. The default is AES128-CTR. Supported algorithms are DES-CBC, 3DES-CBC, AES128-CBC, AES128-CTR, AES128-GCM, AES192-CTR, AES256-CBC, AES256-CTR, and AES256-GCM in ascending order of security strength and computation time.

- **3des-cbc**: Specifies encryption algorithm 3DES-CBC.
- **aes128-cbc**: Specifies encryption algorithm AES128-CBC.
- **aes128-ctr**: Specifies encryption algorithm AES128-CTR.
- **aes128-gcm**: Specifies encryption algorithm AES128-GCM.
- **aes192-ctr**: Specifies encryption algorithm AES192-CTR.
- **aes256-cbc**: Specifies encryption algorithm AES256-CBC.
- **aes256-ctr**: Specifies encryption algorithm AES256-CTR.
- **aes256-gcm**: Specifies encryption algorithm AES256-GCM.
- **des-cbc**: Specifies encryption algorithm DES-CBC.

prefer-ctos-hmac: Specifies the preferred client-to-server HMAC algorithm. The default is SHA2-256. Supported algorithms are MD5, MD5-96, SHA1, SHA1-96, SHA2-256, and SHA2-512 in ascending order of security strength and computation time.

- **md5**: Specifies HMAC algorithm HMAC-MD5.
- **md5-96**: Specifies HMAC algorithm HMAC-MD5-96.
- **sha1**: Specifies HMAC algorithm HMAC-SHA1.
- **sha1-96**: Specifies HMAC algorithm HMAC-SHA1-96.
- **sha2-256**: Specifies HMAC algorithm HMAC-SHA2-256.
- **sha2-512**: Specifies HMAC algorithm HMAC-SHA2-512.

prefer-kex: Specifies the preferred key exchange algorithm. The default is ecdh-sha2-nistp256. Supported algorithms are diffie-hellman-group-exchange-sha1, diffie-hellman-group1-sha1, diffie-hellman-group14-sha1, ecdh-sha2-nistp256, and ecdh-sha2-nistp384, in ascending order of security strength and computation time.

- **dh-group-exchange-sha1**: Specifies key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1-sha1**: Specifies key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14-sha1**: Specifies key exchange algorithm diffie-hellman-group14-sha1.
- **ecdh-sha2-nistp256**: Specifies key exchange algorithm ecdh-sha2-nistp256.
- **ecdh-sha2-nistp384**: Specifies key exchange algorithm ecdh-sha2-nistp384.

prefer-stoc-cipher: Specifies the preferred server-to-client encryption algorithm. The default is AES128-CTR. Supported algorithms are the same as the client-to-server encryption algorithms (see the **prefer-ctos-cipher** keyword).

prefer-stoc-hmac: Specifies the preferred server-to-client HMAC algorithm. The default is SHA2-256. Supported algorithms are the same as the client-to-server HMAC algorithms (see the **prefer-ctos-hmac** keyword).

dscp *dscp-value*: Specifies the DSCP value in the IPv6 SFTP packets. The value range for the *dscp-value* argument is 0 to 63, and the default value is 48. The DSCP value determines the transmission priority of the packet.

public-key *keyname*: Specifies the host public key of the server that the client uses to authenticate the server. The *keyname* argument is a case-insensitive string of 1 to 64 characters.

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

source: Specifies a source IPv6 address or source interface for IPv6 SFTP packets. By default, the device automatically selects a source address for IPv6 SFTP packets in compliance with RFC 3484. As a best practice to ensure successful SFTP connections, specify a loopback interface as the source interface or specify the IPv6 address of a loopback interface as the source address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The IPv6 address of this interface is the source IPv6 address of the IPv6 SFTP packets.
- **ipv6** *ipv6-address*: Specifies a source IPv6 address.

Usage guidelines

If the client and the server have negotiated to use certificate authentication, the client must verify the server's certificate. For the client to correctly get the server's certificate, you must specify the server's PKI domain on the client by using the **server-pki-domain** *domain-name* option. The client uses the CA certificate stored in the specified PKI domain to verify the server's certificate and does not need to save the server's public key before authentication. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

Examples

Connect an SFTP client to SFTP server **2000::1** and specify the public key of the server as **svkey**. The SFTP client uses publickey authentication. Use the following algorithms:

- Preferred key exchange algorithm: **dh-group14-sha1**.
- Preferred server-to-client encryption algorithm: **aes128-cbc**.
- Preferred client-to-server HMAC algorithm: **sha1**.
- Preferred server-to-client HMAC algorithm: **sha1-96**.

- Preferred compression algorithm: **zlib**.

```
<Sysname> sftp ipv6 2000::1 prefer-kex dh-group14-sha1 prefer-stoc-cipher aes128-cbc
prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key svkey
Username:
```

sftp ipv6 suite-b

Use **sftp ipv6 suite-b** to establish a connection to an IPv6 SFTP server based on Suite B algorithms and enter SFTP client view.

Syntax

sftp ipv6 *server* [*port-number*] [**-i** *interface-type interface-number*] **suite-b** [**128-bit** | **192-bit**] **pki-domain** *domain-name* [**server-pki-domain** *domain-name*] [**prefer-compress zlib**] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv6 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range of 1 to 65535. The default is 22.

-i *interface-type interface-number:* Specifies an output interface by its type and number for IPv6 SFTP packets. The specified outgoing interface must have a link-local address. This option is used only when the server uses a link-local address to provide the SFTP service for the client.

suite-b: Specifies the Suite B algorithms. If neither the 128-bit keyword nor the 192-bit keyword is specified, all algorithms in Suite B are used. For more information about the Suite B algorithms, see Table 7.

128-bit: Specifies the 128-bit Suite B security level.

192-bit: Specifies the 192-bit Suite B security level.

pki-domain *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes ('). If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies compression algorithm zlib.

dscp *dscp-value*: Specifies the DSCP value in the IPv6 SFTP packets. The value range for the *dscp-value* argument is 0 to 63, and the default value is 48. The DSCP value determines the transmission priority of the packet.

source: Specifies a source IP address or source interface for IPv6 SFTP packets. By default, the device automatically selects a source address for IPv6 SFTP packets in compliance with RFC 3484. As a best practice to ensure successful SFTP connections, specify a loopback interface as the source interface or specify the IPv6 address of a loopback interface as the source address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The IPv6 address of this interface is the source IP address of the IPv6 SFTP packets.
- **ipv6** *ipv6-address*: Specifies a source IPv6 address.

Usage guidelines

Table 7 Suite B algorithms

Security level	Key exchange algorithm	Encryption algorithm and HMAC algorithm	Public key algorithm
128-bit	ecdh-sha2-nistp256	AES128-GCM	x509v3-ecdsa-sha2-nistp256
192-bit	ecdh-sha2-nistp384	AES256-GCM	x509v3-ecdsa-sha2-nistp384
Both	ecdh-sha2-nistp256 ecdh-sha2-nistp384	AES128-GCM AES256-GCM	x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384

Examples

Use the 192-bit Suite B algorithms to establish a connection to SFTP server **2000::1**. Specify the client's PKI domain and the server's PKI domain as **clientpkidomain** and **serverpkidomain**, respectively.

```
<Sysname> sftp ipv6 2000::1 suite-b 192-bit pki-domain clientpkidomain server-pki-domain
serverpkidomain
Username:
```

sftp suite-b

Use **sftp suite-b** to establish a connection to an IPv4 SFTP server based on Suite B algorithms and enter SFTP client view.

Syntax

sftp *server* [*port-number*] **suite-b** [**128-bit** | **192-bit**] **pki-domain** *domain-name* [**server-pki-domain** *domain-name*] [**prefer-compress zlib**] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv4 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range of 1 to 65535. The default is 22.

suite-b: Specifies the Suite B algorithms. If neither the 128-bit keyword nor the 192-bit keyword is specified, all algorithms in Suite B are used. For more information about the Suite B algorithms, see Table 8.

128-bit: Specifies the 128-bit Suite B security level.

192-bit: Specifies the 192-bit Suite B security level.

pki-domain *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes ('). If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies compression algorithm zlib.

dscp *dscp-value*: Specifies the DSCP value in the IPv4 SFTP packets. The value range for the *dscp-value* argument is 0 to 63, and the default value is 48. The DSCP value determines the transmission priority of the packet.

source: Specifies a source IP address or source interface for the SFTP packets. By default, the device uses the primary IPv4 address of the output interface in the routing entry as the source address of SFTP packets. As a best practice to ensure successful SFTP connections, specify a loopback interface as the source interface or specify the IPv4 address of a loopback interface as the source address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The primary IPv4 address of this interface is the source IPv4 address of the SFTP packets.
- **ip** *ip-address*: Specifies a source IPv4 address.

Usage guidelines

Table 8 Suite B algorithms

Security level	Key exchange algorithm	Encryption algorithm and HMAC algorithm	Public key algorithm
128-bit	ecdh-sha2-nistp256	AES128-GCM	x509v3-ecdsa-sha2-nistp256
192-bit	ecdh-sha2-nistp384	AES256-GCM	x509v3-ecdsa-sha2-nistp384
Both	ecdh-sha2-nistp256 ecdh-sha2-nistp384	AES128-GCM AES256-GCM	x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384

Examples

Use the 128-bit Suite B algorithms to establish a connection to SFTP server **10.1.1.2**. Specify the client's PKI domain and the server's PKI domain as **clientpkidomain** and **serverpkidomain**, respectively.

```
<Sysname> sftp 10.1.1.2 suite-b 128-bit pki-domain clientpkidomain server-pki-domain
serverpkidomain
```

Username

ssh client ipv6 source

Use **ssh client ipv6 source** to configure the source IPv6 address for SSH packets that are sent by the Stelnet client.

Use **undo ssh client ipv6 source** to restore the default.

Syntax

ssh client ipv6 source { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }

undo ssh client ipv6 source

Default

The source IPv6 address for outgoing SSH packets is not configured. The Stelnet client automatically selects an IPv6 address for outgoing SSH packets in compliance with RFC 3484.

Views

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a source interface by its type and number. The Stelnet client selects the interface's address that most specifically matches the destination address of outgoing SSH packets as the source address of the SSH packets.

ipv6 *ipv6-address*: Specifies a source IPv6 address.

Usage guidelines

This command takes effect on all IPv6 Stelnet connections. The source IPv6 address specified in the **ssh2 ipv6** command takes effect only on the current IPv6 Stelnet connection. If you specify the source IPv6 address both in this command and the **ssh2 ipv6** command, the source IPv6 address specified in the **ssh2 ipv6** command takes effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify **2:2::2:2** as the source IPv6 address for SSH packets that are sent by the Stelnet client.

```
<Sysname> system-view
[Sysname] ssh client ipv6 source ipv6 2:2::2:2
```

Related commands

display ssh client source

ssh client source

Use **ssh client source** to configure the source IPv4 address for SSH packets that are sent by the Stelnet client.

Use **undo ssh client source** to restore the default.

Syntax

ssh client source { **interface** *interface-type interface-number* | **ip** *ip-address* }

undo ssh client source

Default

The source IPv4 address for outgoing SSH packets is not configured. The Stelnet client uses the primary IPv4 address of the output interface in the matching route as the source address of outgoing SSH packets.

Views

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a source interface by its type and number. The Stelnet client uses the primary IPv4 address of the interface as the source address of outgoing SSH packets.

ip *ip-address*: Specifies a source IPv4 address.

Usage guidelines

This command takes effect on all Stelnet connections. The source IPv4 address specified in the **ssh2** command takes effect only on the current Stelnet connection. If you specify the source IPv4 address both in this command and the **ssh2** command, the source IPv4 address specified in the **ssh2** command takes effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify **192.168.0.1** as the source IPv4 address for SSH packets.

```
<Sysname> system-view
[Sysname] ssh client source ip 192.168.0.1
```

Related commands

display ssh client source

ssh2

Use **ssh2** to establish a connection to an IPv4 Stelnet server.

Syntax

In non-FIPS mode:

ssh2 *server* [*port-number*] [**identity-key** { **dsa** | **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | { **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } **pki-domain** *domain-name* } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1**

| **sha1-96** | **sha2-256** | **sha2-512** }] * [**dscp** *dscp-value* | **escape** *character* | { **public-key** *keyname* | **server-pki-domain** *domain-name* } | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *

In FIPS mode:

ssh2 *server* [*port-number*] [**identity-key** { **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | { **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } **pki-domain** *domain-name* } | **prefer-compress** **zlib** | **prefer-ctos-cipher** { **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** } | **prefer-ctos-hmac** { **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** } | **prefer-stoc-hmac** { **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [**escape** *character* | { **public-key** *keyname* | **server-pki-domain** *domain-name* } | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv4 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range 1 to 65535. The default is 22.

identity-key: Specifies a public key algorithm for publickey authentication of the client. The default is DSA in non-FIPS mode and is RSA in FIPS mode. If the server uses publickey authentication, you must specify this keyword. The client generates the digital signature or certificate by using the local private key that is associated with the specified algorithm.

- **dsa**: Specifies public key algorithm DSA.
- **ecdsa-sha2-nistp256**: Specifies public key algorithm ecdsa-sha2-nistp256.
- **ecdsa-sha2-nistp384**: Specifies public key algorithm ecdsa-sha2-nistp384.
- **rsa**: Specifies public key algorithm RSA.
- **x509v3-ecdsa-sha2-nistp256**: Specifies public key algorithm x509v3-ecdsa-sha2-nistp256.
- **x509v3-ecdsa-sha2-nistp384**: Specifies public key algorithm x509v3-ecdsa-sha2-nistp384.
- **pki-domain** *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument is a case-insensitive string of 1 to 31 characters. When the x509v3 public key algorithm is used, you must specify this option for the client to get the correct local certificate.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies compression algorithm zlib.

prefer-ctos-cipher: Specifies the preferred client-to-server encryption algorithm. The default is AES128-CTR. Supported algorithms are DES-CBC, 3DES-CBC, AES128-CBC, AES128-CTR, AES128-GCM, AES192-CTR, AES256-CBC, AES256-CTR, and AES256-GCM in ascending order of security strength and computation time.

- **3des-cbc**: Specifies encryption algorithm 3DES-CBC.
- **aes128-cbc**: Specifies encryption algorithm AES128-CBC.
- **aes128-ctr**: Specifies encryption algorithm AES128-CTR.
- **aes128-gcm**: Specifies encryption algorithm AES128-GCM.
- **aes192-ctr**: Specifies encryption algorithm AES192-CTR.
- **aes256-cbc**: Specifies encryption algorithm AES256-CBC.
- **aes256-ctr**: Specifies encryption algorithm AES256-CTR.
- **aes256-gcm**: Specifies encryption algorithm AES256-GCM.
- **des-cbc**: Specifies encryption algorithm DES-CBC.

prefer-ctos-hmac: Specifies the preferred client-to-server HMAC algorithm. The default is SHA2-256. Supported algorithms are MD5, MD5-96, SHA1, SHA1-96, SHA2-256, and SHA2-512 in ascending order of security strength and computation time.

- **md5**: Specifies HMAC algorithm HMAC-MD5.
- **md5-96**: Specifies HMAC algorithm HMAC-MD5-96.
- **sha1**: Specifies HMAC algorithm HMAC-SHA1.
- **sha1-96**: Specifies HMAC algorithm HMAC-SHA1-96.
- **sha2-256**: Specifies HMAC algorithm HMAC-SHA2-256.
- **sha2-512**: Specifies HMAC algorithm HMAC-SHA2-512.

prefer-kex: Specifies the preferred key exchange algorithm. The default is ecdh-sha2-nistp256. Supported algorithms are diffie-hellman-group-exchange-sha1, diffie-hellman-group1-sha1, diffie-hellman-group14-sha1, ecdh-sha2-nistp256, and ecdh-sha2-nistp384, in ascending order of security strength and computation time.

- **dh-group-exchange-sha1**: Specifies key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1-sha1**: Specifies key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14-sha1**: Specifies key exchange algorithm diffie-hellman-group14-sha1.
- **ecdh-sha2-nistp256**: Specifies key exchange algorithm ecdh-sha2-nistp256.
- **ecdh-sha2-nistp384**: Specifies key exchange algorithm ecdh-sha2-nistp384.

prefer-stoc-cipher: Specifies the preferred server-to-client encryption algorithm. The default is AES128-CTR. Supported algorithms are the same as the client-to-server encryption algorithms (see the **prefer-ctos-cipher** keyword).

prefer-stoc-hmac: Specifies the preferred server-to-client HMAC algorithm. The default is SHA2-256. Supported algorithms are the same as the client-to-server HMAC algorithms (see the **prefer-ctos-hmac** keyword).

dscp *dscp-value*: Specifies the DSCP value in the IPv4 SSH packets. The value range for the *dscp-value* argument is 0 to 63, and the default value is 48. The DSCP value determines the transmission priority of the packet.

escape *character*: Specifies a case-sensitive escape character. By default, the escape character is a tilde (~).

public-key *keyname*: Specifies the host public key of the server that the client uses to authenticate the server. The *keyname* argument is a case-insensitive string of 1 to 64 characters.

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive

string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

source: Specifies a source IPv4 address or source interface for SSH packets. By default, the device uses the primary IPv4 address of the output interface in the routing entry as the source address of SSH packets. As a best practice to ensure successful Stelnet connections, specify a loopback interface as the source interface or specify the IPv4 address of a loopback interface as the source address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The primary IPv4 address of this interface is the source IPv4 address of the SSH packets.
- **ip** *ip-address*: Specifies a source IPv4 address.

Usage guidelines

The combination of an escape character and a dot (.) works as an escape sequence. This escape sequence is typically used to quickly terminate an SSH connection when the server reboots or malfunctions.

For the escape sequence to take effect, you must enter it at the very beginning of a line. If you have entered other characters or performed operations in a line, enter the escape sequence in the next line.

As a best practice, use the default escape character (~). Do not use any character in SSH usernames as the escape character.

If the client and the server have negotiated to use certificate authentication, the client must verify the server's certificate. For the client to correctly get the server's certificate, you must specify the server's PKI domain on the client by using the **server-pki-domain** *domain-name* option. The client uses the CA certificate stored in the specified PKI domain to verify the server's certificate and does not need to save the server's public key before authentication. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

Examples

Establish a connection to Stelnet server **3.3.3.3** and specify the public key of the server as **svkey**. The Stelnet client uses publickey authentication. Specify the dollar sign ($) as the escape character. Use the following algorithms:

- Preferred key exchange algorithm: **dh-group14-sha1**.
- Preferred server-to-client encryption algorithm: **aes128-cbc**.
- Preferred client-to-server HMAC algorithm: **sha1**.
- Preferred server-to-client HMAC algorithm: **sha1-96**.
- Preferred compression algorithm: **zlib**.

```
<Sysname> ssh2 3.3.3.3 prefer-kex dh-group14-sha1 prefer-stoc-cipher aes128-cbc
prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key svkey
escape $
```

ssh2 ipv6

Use **ssh2 ipv6** to establish a connection to an IPv6 Stelnet server.

Syntax

In non-FIPS mode:

ssh2 ipv6 *server* [*port-number*] [**-i** *interface-type interface-number*] [**identity-key** { **dsa** | **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | { **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } **pki-domain** *domain-name* } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** |

aes128-cbc | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [**dscp** *dscp-value* | **escape** *character* | { **public-key** *keyname* | **server-pki-domain** *domain-name* } | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

In FIPS mode:

ssh2 ipv6 *server* [*port-number*] [**-i** *interface-type interface-number*] [**identity-key** { **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | { **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } **pki-domain** *domain-name* } | **prefer-compress zlib** | **prefer-ctos-cipher** { **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** } | **prefer-ctos-hmac** { **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** } | **prefer-stoc-hmac** { **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [**escape** *character* | { **public-key** *keyname* | **server-pki-domain** *domain-name* } | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv6 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range 1 to 65535. The default is 22.

-i *interface-type interface-number:* Specifies an output interface by its type and number for IPv6 SSH packets. This option is used only when the server uses a link-local address to provide the Stelnet service for the client. The specified output interface on the Stelnet client must have a link-local address.

identity-key: Specifies a public key algorithm for publickey authentication of the client. The default is DSA in non-FIPS mode and is RSA in FIPS mode. If the server uses publickey authentication, you must specify this keyword. The client generates the digital signature or certificate by using the local private key that is associated with the specified algorithm.

- **dsa**: Specifies public key algorithm DSA.
- **ecdsa-sha2-nistp256**: Specifies public key algorithm ecdsa-sha2-nistp256.
- **ecdsa-sha2-nistp384**: Specifies public key algorithm ecdsa-sha2-nistp384.
- **rsa**: Specifies public key algorithm RSA.
- **x509v3-ecdsa-sha2-nistp256**: Specifies public key algorithm x509v3-ecdsa-sha2-nistp256.
- **x509v3-ecdsa-sha2-nistp384**: Specifies public key algorithm x509v3-ecdsa-sha2-nistp384.

- **pki-domain** *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument is a case-insensitive string of 1 to 31 characters. When the x509v3 public key algorithm is used, you must specify this option for the client to get the correct local certificate.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies compression algorithm zlib.

prefer-ctos-cipher: Specifies the preferred client-to-server encryption algorithm. The default is AES128-CTR. Supported algorithms are DES-CBC, 3DES-CBC, AES128-CBC, AES128-CTR, AES128-GCM, AES192-CTR, AES256-CBC, AES256-CTR, and AES256-GCM in ascending order of security strength and computation time.

- **3des-cbc**: Specifies encryption algorithm 3DES-CBC.
- **aes128-cbc**: Specifies encryption algorithm AES128-CBC.
- **aes128-ctr**: Specifies encryption algorithm AES128-CTR.
- **aes128-gcm**: Specifies encryption algorithm AES128-GCM.
- **aes192-ctr**: Specifies encryption algorithm AES192-CTR.
- **aes256-cbc**: Specifies encryption algorithm AES256-CBC.
- **aes256-ctr**: Specifies encryption algorithm AES256-CTR.
- **aes256-gcm**: Specifies encryption algorithm AES256-GCM.
- **des-cbc**: Specifies encryption algorithm DES-CBC.

prefer-ctos-hmac: Specifies the preferred client-to-server HMAC algorithm. The default is SHA2-256. Supported algorithms are MD5, MD5-96, SHA1, SHA1-96, SHA2-256, and SHA2-512 in ascending order of security strength and computation time.

- **md5**: Specifies HMAC algorithm HMAC-MD5.
- **md5-96**: Specifies HMAC algorithm HMAC-MD5-96.
- **sha1**: Specifies HMAC algorithm HMAC-SHA1.
- **sha1-96**: Specifies HMAC algorithm HMAC-SHA1-96.
- **sha2-256**: Specifies HMAC algorithm HMAC-SHA2-256.
- **sha2-512**: Specifies HMAC algorithm HMAC-SHA2-512.

prefer-kex: Specifies the preferred key exchange algorithm. The default is ecdh-sha2-nistp256. Supported algorithms are diffie-hellman-group-exchange-sha1, diffie-hellman-group1-sha1, diffie-hellman-group14-sha1, ecdh-sha2-nistp256, and ecdh-sha2-nistp384, in ascending order of security strength and computation time.

- **dh-group-exchange-sha1**: Specifies key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1-sha1**: Specifies key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14-sha1**: Specifies key exchange algorithm diffie-hellman-group14-sha1.
- **ecdh-sha2-nistp256**: Specifies key exchange algorithm ecdh-sha2-nistp256.
- **ecdh-sha2-nistp384**: Specifies key exchange algorithm ecdh-sha2-nistp384.

prefer-stoc-cipher: Specifies the preferred server-to-client encryption algorithm. The default is AES128-CTR. Supported algorithms are the same as the client-to-server encryption algorithms (see the **prefer-ctos-cipher** keyword).

prefer-stoc-hmac: Specifies the preferred server-to-client HMAC algorithm. The default is SHA2-256. Supported algorithms are the same as the client-to-server HMAC algorithms (see the **prefer-ctos-hmac** keyword).

dscp *dscp-value*: Specifies the DSCP value in the IPv6 SSH packets. The value range for the *dscp-value* argument is 0 to 63, and the default value is 48. The DSCP value determines the transmission priority of the packet.

escape *character*: Specifies a case-sensitive escape character. By default, the escape character is a tilde (~).

public-key *keyname*: Specifies the server by its host public key that the client uses to authenticate the server. The *keyname* argument is a case-insensitive string of 1 to 64 characters.

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

source: Specifies a source IPv6 address or source interface for IPv6 SSH packets. By default, the device automatically selects a source address for IPv6 SSH packets in compliance with RFC 3484. As a best practice to ensure successful Stelnet connections, specify a loopback interface as the source interface or specify the IPv6 address of a loopback interface as the source address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The IPv6 address of this interface is the source IPv6 address of the IPv6 SSH packets.
- **ipv6** *ipv6-address*: Specifies a source IPv6 address.

Usage guidelines

The combination of an escape character and a dot (.) works as an escape sequence. This escape sequence is typically used to quickly terminate an SSH connection when the server reboots or malfunctions.

For the escape sequence to take effect, you must enter it at the very beginning of a line. If you have entered other characters or performed operations in a line, enter the escape sequence in the next line.

As a best practice, use the default escape character (~). Do not use any characters in SSH usernames as the escape character.

If the client and the server have negotiated to use certificate authentication, the client must verify the server's certificate. For the client to correctly get the server's certificate, you must specify the server's PKI domain on the client by using the **server-pki-domain** *domain-name* option. The client uses the CA certificate stored in the specified PKI domain to verify the server's certificate and does not need to save the server's public key before authentication. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

Examples

Establish a connection to Stelnet server **2000::1** and specify the public key of the server as **svkey**. The SSH client uses publickey authentication. Specify the dollar sign ($) as the escape character. Use the following algorithms:

- Preferred key exchange algorithm: **dh-group14-sha1**.
- Preferred server-to-client encryption algorithm: **aes128-cbc**.
- Preferred client-to-server HMAC algorithm: **sha1**.
- Preferred server-to-client HMAC algorithm: **sha1-96**.
- Preferred compression algorithm: **zlib**.

```
<Sysname> ssh2 ipv6 2000::1 prefer-kex dh-group14-sha1 prefer-stoc-cipher aes128-cbc
prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key svkey
escape $
```

ssh2 ipv6 suite-b

Use **ssh2 ipv6 suite-b** to establish a connection to an IPv6 Stelnet server based on Suite B algorithms.

Syntax

ssh2 ipv6 *server* [*port-number*] [**-i** *interface-type interface-number*] **suite-b** [**128-bit** | **192-bit**] **pki-domain** *domain-name* [**server-pki-domain** *domain-name*] [**prefer-compress zlib**] [**dscp** *dscp-value* | **escape** *character* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv6 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range 1 to 65535. The default is 22.

-i *interface-type interface-number:* Specifies an output interface by its type and number for IPv6 SSH packets. Specify this option when the server uses a link-local address to provide the Stelnet service for the client. The specified output interface on the Stelnet client must have a link-local address.

suite-b: Specifies the Suite B algorithms. If neither the 128-bit keyword nor the 192-bit keyword is specified, all algorithms in Suite B are used. For more information about the Suite B algorithms, see Table 9.

128-bit: Specifies the 128-bit Suite B security level.

192-bit: Specifies the 192-bit Suite B security level.

pki-domain *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes ('). If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies compression algorithm zlib.

dscp *dscp-value*: Specifies the DSCP value in the IPv6 SSH packets. The value range for the *dscp-value* argument is 0 to 63, and the default value is 48. The DSCP value determines the transmission priority of the packet.

escape *character*: Specifies a case-sensitive escape character. By default, the escape character is a tilde (~).

source: Specifies a source IP address or source interface for IPv6 SSH packets. By default, the device automatically selects a source address for IPv6 SSH packets in compliance with RFC 3484. As a best practice to ensure successful Stelnet connections, specify a loopback interface as the source interface or specify the IPv6 address of a loopback interface as the source address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The IPv6 address of this interface is the source IP address of the IPv6 SSH packets.
- **ipv6** *ipv6-address*: Specifies a source IPv6 address.

Usage guidelines

Table 9 Suite B algorithms

Security level	Key exchange algorithm	Encryption algorithm and HMAC algorithm	Public key algorithm
128-bit	ecdh-sha2-nistp256	AES128-GCM	x509v3-ecdsa-sha2-nistp256
192-bit	ecdh-sha2-nistp384	AES256-GCM	x509v3-ecdsa-sha2-nistp384
Both	ecdh-sha2-nistp256 ecdh-sha2-nistp384	AES128-GCM AES256-GCM	x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384

The combination of an escape character and a dot (.) works as an escape sequence. This escape sequence is typically used to quickly terminate an SSH connection when the server reboots or malfunctions.

For the escape sequence to take effect, you must enter it at the very beginning of a line. If you have entered other characters or performed operations in a line, enter the escape sequence in the next line. As a best practice, use the default escape character (~). Do not use any character in SSH usernames as the escape character.

Examples

Use the 192-bit Suite B algorithms to establish a connection to Stelnet server **2000::1**. Specify the client's PKI domain and the server's PKI domain as **clientpkidomain** and **serverpkidomain**, respectively.

```
<Sysname> ssh2 ipv6 2000::1 suite-b 192-bit pki-domain clientpkidomain server-pki-domain
serverpkidomain
Username
```

ssh2 suite-b

Use **ssh2 suite-b** to establish a connection to an IPv4 Stelnet server based on Suite B algorithms.

Syntax

ssh2 *server* [*port-number*] **suite-b** [**128-bit** | **192-bit**] **pki-domain** *domain-name* [**server-pki-domain** *domain-name*] [**prefer-compress zlib**] [**dscp** *dscp-value* | **escape** *character* | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv4 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range 1 to 65535. The default is 22.

suite-b: Specifies the Suite B algorithms. If neither the 128-bit keyword nor the 192-bit keyword is specified, all algorithms in Suite B are used. For more information about the Suite B algorithms, see Table 10.

128-bit: Specifies the 128-bit Suite B security level.

192-bit: Specifies the 192-bit Suite B security level.

pki-domain *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes ('). If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies compression algorithm zlib.

dscp *dscp-value*: Specifies the DSCP value in the IPv4 SSH packets. The value range for the *dscp-value* argument is 0 to 63, and the default value is 48. The DSCP value determines the transmission priority of the packet.

escape *character*: Specifies a case-sensitive escape character. By default, the escape character is a tilde (~).

source: Specifies a source IP address or source interface for SSH packets. By default, the device uses the primary IPv4 address of the output interface in the routing entry as the source address of SSH packets. As a best practice to ensure successful Stelnet connections, specify a loopback interface as the source interface or specify the IPv4 address a loopback interface as the source address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The primary IPv4 address of this interface is the source IPv4 address of the SSH packets.
- **ip** *ip-address*: Specifies a source IPv4 address.

Usage guidelines

Table 10 Suite B algorithms

Security level	Key exchange algorithm	Encryption algorithm and HMAC algorithm	Public key algorithm
128-bit	ecdh-sha2-nistp256	AES128-GCM	x509v3-ecdsa-sha2-nistp256
192-bit	ecdh-sha2-nistp384	AES256-GCM	x509v3-ecdsa-sha2-nistp384
Both	ecdh-sha2-nistp256	AES128-GCM	x509v3-ecdsa-sha2-nistp256

Security level	Key exchange algorithm	Encryption algorithm and HMAC algorithm	Public key algorithm
	ecdh-sha2-nistp384	AES256-GCM	x509v3-ecdsa-sha2-nistp384

The combination of an escape character and a dot (.) works as an escape sequence. This escape sequence is typically used to quickly terminate an SSH connection when the server reboots or malfunctions.

For the escape sequence to take effect, you must enter it at the very beginning of a line. If you have entered other characters or performed operations in a line, enter the escape sequence in the next line. As a best practice, use the default escape character (~). Do not use any character in SSH usernames as the escape character.

Examples

Use the 128-bit Suite B algorithms to establish a connection to Stelnet server **3.3.3.3**. Specify the client's PKI domain and the server's PKI domain as **clientpkidomain** and **serverpkidomain**, respectively.

```
<Sysname> ssh2 3.3.3.3 suite-b 128-bit pki-domain clientpkidomain server-pki-domain
serverpkidomain
Username
```

SSH2 commands

display ssh2 algorithm

Use **`display ssh2 algorithm`** to display algorithms used by SSH2 in the algorithm negotiation stage.

Syntax

`display ssh2 algorithm`

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display algorithms used by SSH2 in the algorithm negotiation stage.

```
<Sysname> display ssh2 algorithm
 Key exchange algorithms: ecdh-sha2-nistp256 ecdh-sha2-nistp384 dh-group-exchange-sha1
dh-group14-sha1 dh-group1-sha1
 Public key algorithms: x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384
ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 rsa dsa
 Encryption algorithms: aes128-ctr aes192-ctr aes256-ctr aes128-gcm aes256-gcm aes128-cbc
3des-cbc aes256-cbc des-cbc
 MAC algorithms: sha2-256 sha2-512 sha1 md5 sha1-96 md5-96
```

Table 11 Command output

Field	Description
Key exchange algorithms	Key exchange algorithms in descending order of priority for algorithm negotiation.
Public key algorithms	Public key algorithms in descending order of priority for algorithm negotiation.
Encryption algorithms	Encryption algorithms in descending order of priority for algorithm negotiation.
MAC algorithms	HMAC algorithms in descending order of priority for algorithm negotiation.

Related commands

ssh2 algorithm cipher

ssh2 algorithm key-exchange

ssh2 algorithm mac

ssh2 algorithm public-key

ssh2 algorithm cipher

Use **ssh2 algorithm cipher** to specify encryption algorithms for SSH2.

Use **undo ssh2 algorithm cipher** to restore the default.

Syntax

In non-FIPS mode:

ssh2 algorithm cipher { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } *

undo ssh2 algorithm cipher

In FIPS mode:

ssh2 algorithm cipher { **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** } *

undo ssh2 algorithm cipher

Default

SSH2 uses encryption algorithms AES128-CTR, AES192-CTR, AES256-CTR, AES128-GCM, AES256-GCM, AES128-CBC, 3DES-CBC, AES256-CBC, and DES-CBC in descending order of priority for algorithm negotiation.

Views

System view

Predefined user roles

network-admin

Parameters

3des-cbc: Specifies encryption algorithm 3DES-CBC.

aes128-cbc: Specifies encryption algorithm AES128-CBC.

aes128-ctr: Specifies encryption algorithm AES128-CTR.

aes128-gcm: Specifies encryption algorithm AES128-GCM.

aes192-ctr: Specifies encryption algorithm AES192-CTR.

aes256-cbc: Specifies encryption algorithm AES256-CBC.

aes256-ctr: Specifies encryption algorithm AES256-CTR.

aes256-gcm: Specifies encryption algorithm AES256-GCM.

des-cbc: Specifies encryption algorithm DES-CBC.

Usage guidelines

If you specify the encryption algorithms, SSH2 uses only the specified algorithms for algorithm negotiation. The algorithm specified earlier has a higher priority during negotiation.

Examples

Specify algorithm **aes256-cbc** as the encryption algorithm for SSH2.

```
<Sysname> system-view
[Sysname] ssh2 algorithm cipher aes256-cbc
```

Related commands

display ssh2 algorithm

ssh2 algorithm key-exchange

ssh2 algorithm mac

ssh2 algorithm public-key

ssh2 algorithm key-exchange

Use **ssh2 algorithm key-exchange** to specify key exchange algorithms for SSH2.

Use **undo ssh2 algorithm key-exchange** to restore the default.

Syntax

In non-FIPS mode:

ssh2 algorithm key-exchange { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } *

undo ssh2 algorithm key-exchange

In FIPS mode:

ssh2 algorithm key-exchange { **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } *

undo ssh2 algorithm key-exchange

Default

SSH2 uses key exchange algorithms ecdh-sha2-nistp256, ecdh-sha2-nistp384, diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, and diffie-hellman-group1-sha1 in descending order of priority for algorithm negotiation.

Views

System view

Predefined user roles

network-admin

Parameters

dh-group-exchange-sha1: Specifies key exchange algorithm diffie-hellman-group-exchange-sha1.

dh-group1-sha1: Specifies key exchange algorithm diffie-hellman-group1-sha1.

dh-group14-sha1: Specifies key exchange algorithm diffie-hellman-group14-sha1.

ecdh-sha2-nistp256: Specifies key exchange algorithm ecdh-sha2-nistp256.

ecdh-sha2-nistp384: Specifies key exchange algorithm ecdh-sha2-nistp384.

Usage guidelines

If you specify the key exchange algorithms, SSH2 uses only the specified algorithms for algorithm negotiation. The algorithm specified earlier has a higher priority during negotiation.

Examples

Specify algorithm **dh-group1-sha1** as the key exchange algorithm for SSH2.

```
<Sysname> system-view
[Sysname] ssh2 algorithm key-exchange dh-group1-sha1
```

Related commands

display ssh2 algorithm

ssh2 algorithm cipher

ssh2 algorithm mac

ssh2 algorithm public-key

ssh2 algorithm mac

Use **ssh2 algorithm mac** to specify HMAC algorithms for SSH2.

Use **undo ssh2 algorithm mac** to restore the default.

Syntax

In non-FIPS mode:

ssh2 algorithm mac { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } *

undo ssh2 algorithm mac

In FIPS mode:

ssh2 algorithm mac { **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } *

undo ssh2 algorithm mac

Default

SSH2 uses HMAC algorithms SHA2-256, SHA2-512, SHA1, MD5, SHA1-96, and MD5-96 in descending order of priority for algorithm negotiation.

Views

System view

Predefined user roles

network-admin

Parameters

md5: Specifies HMAC algorithm HMAC-MD5.

md5-96: Specifies HMAC algorithm HMAC-MD5-96.

sha1: Specifies HMAC algorithm HMAC-SHA1.

sha1-96: Specifies HMAC algorithm HMAC-SHA1-96.

sha2-256: Specifies HMAC algorithm HMAC-SHA2-256.

sha2-512: Specifies HMAC algorithm HMAC-SHA2-512.

Usage guidelines

If you specify the HMAC algorithms, SSH2 uses only the specified algorithms for algorithm negotiation. The algorithm specified earlier has a higher priority during negotiation.

Examples

Specify algorithm **md5** as the HMAC algorithm for SSH2.

```
<Sysname> system-view
[Sysname] ssh2 algorithm mac md5
```

Related commands

display ssh2 algorithm

ssh2 algorithm cipher

ssh2 algorithm key-exchange

ssh2 algorithm public-key

ssh2 algorithm public-key

Use **ssh2 algorithm public-key** to specify public key algorithms for SSH2.

Use **undo ssh2 algorithm public-key** to restore the default.

Syntax

In non-FIPS mode:

ssh2 algorithm public-key { dsa | ecdsa-sha2-nistp256 | ecdsa-sha2-nistp384 | rsa | x509v3-ecdsa-sha2-nistp256 | x509v3-ecdsa-sha2-nistp384 } *

undo ssh2 algorithm public-key

In FIPS mode:

ssh2 algorithm public-key { ecdsa-sha2-nistp256 | ecdsa-sha2-nistp384 | rsa | x509v3-ecdsa-sha2-nistp256 | x509v3-ecdsa-sha2-nistp384 } *

undo ssh2 algorithm public-key

Default

SSH2 uses public key algorithms x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, RSA, and DSA in descending order of priority for algorithm negotiation.

Views

System view

Predefined user roles

network-admin

Parameters

dsa: Specifies public key algorithm DSA.

ecdsa-sha2-nistp256: Specifies public key algorithm ecdsa-sha2-nistp256.

ecdsa-sha2-nistp384: Specifies public key algorithm ecdsa-sha2-nistp384.

rsa: Specifies public key algorithm RSA.

x509v3-ecdsa-sha2-nistp256: Specifies public key algorithm x509v3-ecdsa-sha2-nistp256.

x509v3-ecdsa-sha2-nistp384: Specifies public key algorithm x509v3-ecdsa-sha2-nistp384.

Usage guidelines

If you specify the public key algorithms, SSH2 uses only the specified algorithms for algorithm negotiation. The algorithm specified earlier has a higher priority during negotiation.

Examples

Specify algorithm **dsa** as the public key algorithm for SSH2.

```
<Sysname> system-view
[Sysname] ssh2 algorithm public-key dsa
```

Related commands

display ssh2 algorithm

ssh2 algorithm cipher

ssh2 algorithm key-exchange

ssh2 algorithm mac

Contents

SSL commands

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

certificate-chain-sending enable

Use **certificate-chain-sending enable** to enable the SSL server to send the complete certificate chain to the client during SSL negotiation.

Use **undo certificate-chain-sending enable** to restore the default.

Syntax

certificate-chain-sending enable

undo certificate-chain-sending enable

Default

During SSL negotiation, the SSL server sends the server certificate rather than the complete certificate chain to the client.

Views

SSL server policy view

Predefined user roles

network-admin

Usage guidelines

This feature causes additional overheads in the SSL negotiation process. Enable it only when the SSL client does not have the complete certificate chain to verify the server certificate.

Examples

Enable the SSL server to send the complete certificate chain to the client during SSL negotiation.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] certificate-chain-sending enable
```

Related commands

display ssl server-policy

ciphersuite

Use **ciphersuite** to specify the cipher suites supported by an SSL server policy.

Use **undo ciphersuite** to restore the default.

Syntax

In non-FIPS mode:

ciphersuite { dhe_rsa_aes_128_cbc_sha | dhe_rsa_aes_128_cbc_sha256 | dhe_rsa_aes_256_cbc_sha | dhe_rsa_aes_256_cbc_sha256 | ecdhe_ecdsa_aes_128_cbc_sha256 | ecdhe_ecdsa_aes_128_gcm_sha256 | ecdhe_ecdsa_aes_256_cbc_sha384 | ecdhe_ecdsa_aes_256_gcm_sha384 | ecdhe_rsa_aes_128_cbc_sha256 | ecdhe_rsa_aes_128_gcm_sha256 |

ecdhe_rsa_aes_256_cbc_sha384 | **ecdhe_rsa_aes_256_gcm_sha384** | **exp_rsa_des_cbc_sha** | **exp_rsa_rc2_md5** | **exp_rsa_rc4_md5** | **rsa_3des_ede_cbc_sha** | **rsa_aes_128_cbc_sha** | **rsa_aes_128_cbc_sha256** | **rsa_aes_256_cbc_sha** | **rsa_aes_256_cbc_sha256** | **rsa_des_cbc_sha** | **rsa_rc4_128_md5** | **rsa_rc4_128_sha** } *

undo ciphersuite

In FIPS mode:

ciphersuite { **ecdhe_ecdsa_aes_128_cbc_sha256** | **ecdhe_ecdsa_aes_256_cbc_sha384** | **ecdhe_ecdsa_aes_128_gcm_sha256** | **ecdhe_ecdsa_aes_256_gcm_sha384** | **ecdhe_rsa_aes_128_cbc_sha256** | **ecdhe_rsa_aes_128_gcm_sha256** | **ecdhe_rsa_aes_256_cbc_sha384** | **ecdhe_rsa_aes_256_gcm_sha384** | **rsa_aes_128_cbc_sha** | **rsa_aes_128_cbc_sha256** | **rsa_aes_256_cbc_sha** | **rsa_aes_256_cbc_sha256** } *

undo ciphersuite

Default

An SSL server policy supports all cipher suites.

Views

SSL server policy view

Predefined user roles

network-admin

Parameters

dhe_rsa_aes_128_cbc_sha: Specifies the cipher suite that uses key exchange algorithm DHE RSA, data encryption algorithm 128-bit AES_CBC, and MAC algorithm SHA.

dhe_rsa_aes_128_cbc_sha256: Specifies the cipher suite that uses key exchange algorithm DHE RSA, data encryption algorithm 128-bit AES_CBC, and MAC algorithm SHA256.

dhe_rsa_aes_256_cbc_sha: Specifies the cipher suite that uses key exchange algorithm DHE RSA, data encryption algorithm 256-bit AES_CBC, and MAC algorithm SHA.

dhe_rsa_aes_256_cbc_sha256: Specifies the cipher suite that uses key exchange algorithm DHE RSA, data encryption algorithm 256-bit AES_CBC, and MAC algorithm SHA256.

ecdhe_ecdsa_aes_128_cbc_sha256: Specifies the cipher suite that uses key exchange algorithm ECDHE ECDSA, data encryption algorithm 128-bit AES_CBC, and MAC algorithm SHA256.

ecdhe_ecdsa_aes_128_gcm_sha256: Specifies the cipher suite that uses key exchange algorithm ECDHE ECDSA, data encryption algorithm 128-bit AES_GCM, and MAC algorithm SHA256.

ecdhe_ecdsa_aes_256_cbc_sha384: Specifies the cipher suite that uses key exchange algorithm ECDHE ECDSA, data encryption algorithm 256-bit AES_CBC, and MAC algorithm SHA384.

ecdhe_ecdsa_aes_256_gcm_sha384: Specifies the cipher suite that uses key exchange algorithm ECDHE ECDSA, data encryption algorithm 256-bit AES_GCM, and MAC algorithm SHA384.

ecdhe_rsa_aes_128_cbc_sha256: Specifies the cipher suite that uses key exchange algorithm ECDHE RSA, data encryption algorithm 128-bit AES_CBC, and MAC algorithm SHA256.

ecdhe_rsa_aes_128_gcm_sha256: Specifies the cipher suite that uses key exchange algorithm ECDHE RSA, data encryption algorithm 128-bit AES_GCM, and MAC algorithm SHA256.

ecdhe_rsa_aes_256_cbc_sha384: Specifies the cipher suite that uses key exchange algorithm ECDHE RSA, data encryption algorithm 256-bit AES_CBC, and MAC algorithm SHA384.

ecdhe_rsa_aes_256_gcm_sha384: Specifies the cipher suite that uses key exchange algorithm ECDHE RSA, data encryption algorithm 256-bit AES_GCM, and MAC algorithm SHA384.

exp_rsa_des_cbc_sha: Specifies the export cipher suite that uses key exchange algorithm RSA, data encryption algorithm DES_CBC, and MAC algorithm SHA.

exp_rsa_rc2_md5: Specifies the export cipher suite that uses key exchange algorithm RSA, data encryption algorithm RC2, and MAC algorithm MD5.

exp_rsa_rc4_md5: Specifies the export cipher suite that uses key exchange algorithm RSA, data encryption algorithm RC4, and MAC algorithm MD5.

rsa_3des_ede_cbc_sha: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm 3DES_EDE_CBC, and MAC algorithm SHA.

rsa_aes_128_cbc_sha: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm 128-bit AES_CBC, and MAC algorithm SHA.

rsa_aes_128_cbc_ sha256: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm 128-bit AES_CBC, and MAC algorithm SHA256.

rsa_aes_256_cbc_sha: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm 256-bit AES_CBC, and MAC algorithm SHA.

rsa_aes_256_cbc_ sha256: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm 256-bit AES_CBC, and MAC algorithm SHA256.

rsa_des_cbc_sha: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm DES_CBC, and MAC algorithm SHA.

rsa_rc4_128_md5: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm 128-bit RC4, and MAC algorithm MD5.

rsa_rc4_128_sha: Specifies key exchange algorithm RSA, data encryption algorithm 128-bit RC4, and MAC algorithm SHA.

Usage guidelines

SSL employs the following algorithms:

- **Data encryption algorithms**—Encrypt data to ensure privacy. Commonly used data encryption algorithms are symmetric key algorithms. When a symmetric key algorithm is used, the SSL server and the SSL client must use the same key.
- **Message Authentication Code (MAC) algorithms**—Calculate the MAC value for data to ensure integrity. Commonly used MAC algorithms include MD5 and SHA. When a MAC algorithm is used, the SSL server and the SSL client must use the same key.
- **Key exchange algorithms**—Implement secure exchange of the keys used by the symmetric key algorithm and the MAC algorithm. Commonly used key exchange algorithms are usually asymmetric key algorithms, such as RSA.

After the SSL server receives a cipher suite from a client, the server matches the received cipher suite against the cipher suits it supports. If a match is found, the cipher suite negotiation succeeds. Otherwise, the negotiation fails.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure SSL server policy **policy1** to support the following cipher suites:

- Key exchange algorithm DHE RSA, data encryption algorithm 128-bit AES, and MAC algorithm SHA.
- Key exchange algorithm RSA, data encryption algorithm 128-bit AES, and MAC algorithm SHA.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] ciphersuite dhe_rsa_aes_128_cbc_sha
rsa_aes_128_cbc_sha
```

Related commands

display ssl server-policy

prefer-cipher

client-verify

Use **client-verify** to enable mandatory or optional SSL client authentication.

Use **undo client-verify** to restore the default.

Syntax

client-verify { **enable** | **optional** }

undo client-verify [**enable**]

Default

SSL client authentication is disabled. The SSL server does not authenticate SSL clients based on digital certificates.

Views

SSL server policy view

Predefined user roles

network-admin

Parameters

enable: Enables mandatory SSL client authentication.

optional: Enables optional SSL client authentication.

Usage guidelines

SSL uses digital certificates to authenticate communicating parties. For more information about digital certificates, see *Security Configuration Guide*.

Mandatory SSL client authentication—The SSL server requires an SSL client to submit its digital certificate for identity authentication. The SSL client can access the SSL server only after it passes identity authentication.

Optional SSL client authentication—The SSL server does not require an SSL client to submit its digital certificate for identity authentication.

- If an SSL client submits its certificate to the SSL server, the server authenticates the client identity. The client must pass authentication to access the server.
- If an SSL client does not submit its certificate to the SSL server, the server does not authenticate the client identity. The client can access the SSL server without authentication.

If SSL client authentication is disabled, the SSL server does not authenticate SSL clients regardless of whether the clients submit digital certificates or not. SSL clients can access the SSL server without authentication.

When authenticating a client by using the digital certificate, the SSL server performs the following operations:

- Verifies the certificate chain presented by the client.

- Checks that the certificates in the certificate chain (except the root CA certificate) are not revoked.

Examples

Enable mandatory SSL client authentication.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] client-verify enable
```

Enable optional SSL client authentication.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] client-verify optional
```

Disable SSL client authentication.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] undo client-verify
```

Related commands

display ssl server-policy

display ssl client-policy

Use **display ssl client-policy** to display SSL client policy information.

Syntax

display ssl client-policy [*policy-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

policy-name: Specifies an SSL client policy by its name, a case-insensitive string of 1 to 31 characters. If you do not specify a policy name, this command displays information about all SSL client policies.

Examples

Display information about the SSL client policy **policy1**.

```
<Sysname> display ssl client-policy policy1
 SSL client policy: policy1
     SSL version: SSL 3.0
     PKI domain: client-domain
     Preferred ciphersuite:
         RSA_AES_128_CBC_SHA
     Server-verify: enabled
```

Table 1 Command output

Field	Description
Server-verify	Indicates whether the client is enabled to use digital certificates to authenticate servers.

display ssl server-policy

Use **display ssl server-policy** to display SSL server policy information.

Syntax

display ssl server-policy [*policy-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

policy-name: Specifies an SSL server policy by its name, a case-insensitive string of 1 to 31 characters. If you do not specify a policy name, this command displays information about all SSL server policies.

Examples

Display information about the SSL server policy **policy1**.

```
<Sysname> display ssl server-policy policy1
 SSL server policy: policy1
     PKI domain: server-domain
     Ciphersuites:
         DHE_RSA_AES_128_CBC_SHA
         RSA_AES_128_CBC_SHA
     Session cache size: 600
     Caching timeout: 3600 seconds
     Client-verify: Enabled
     Certificate chain sending: Enabled
```

Table 2 Command output

Field	Description
Caching timeout	Session cache timeout time in seconds.
Client-verify	SSL client authentication mode, including: • **Disabled**—SSL client authentication is disabled. • **Enabled**—SSL client authentication is mandatory. • **Optional**—SSL client authentication is optional.
Certificate chain sending	Whether the SSL server is enabled to send the complete certificate chain to the client during SSL negotiation.

pki-domain (SSL client policy view)

Use **pki-domain** to specify a PKI domain for an SSL client policy.

Use **undo pki-domain** to restore the default.

Syntax

pki-domain *domain-name*

undo pki-domain

Default

No PKI domain is specified for an SSL client policy.

Views

SSL client policy view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

If you specify a PKI domain for an SSL client policy, the SSL client that uses the SSL client policy will obtain its digital certificate through the specified PKI domain.

Examples

Specify PKI domain **client-domain** for SSL client policy **policy1**.

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1] pki-domain client-domain
```

Related commands

display ssl client-policy

pki domain

pki-domain (SSL server policy view)

Use **pki-domain** to specify a PKI domain for an SSL server policy.

Use **undo pki-domain** to restore the default.

Syntax

pki-domain *domain-name*

undo pki-domain

Default

No PKI domain is specified for an SSL server policy.

Views

SSL server policy view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

If you specify a PKI domain for an SSL server policy, the SSL server that uses the SSL server policy will obtain its digital certificate through the specified PKI domain.

Examples

Specify PKI domain **server-domain** for SSL server policy **policy1**.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] pki-domain server-domain
```

Related commands

display ssl server-policy

pki domain

prefer-cipher

Use **prefer-cipher** to specify a preferred cipher suite for an SSL client policy.

Use **undo prefer-cipher** to restore the default.

Syntax

In non-FIPS mode:

prefer-cipher { **dhe_rsa_aes_128_cbc_sha** | **dhe_rsa_aes_128_cbc_sha256** | **dhe_rsa_aes_256_cbc_sha** | **dhe_rsa_aes_256_cbc_sha256** | **ecdhe_ecdsa_aes_128_cbc_sha256** | **ecdhe_ecdsa_aes_128_gcm_sha256** | **ecdhe_ecdsa_aes_256_cbc_sha384** | **ecdhe_ecdsa_aes_256_gcm_sha384** | **ecdhe_rsa_aes_128_cbc_sha256** | **ecdhe_rsa_aes_128_gcm_sha256** | **ecdhe_rsa_aes_256_cbc_sha384** | **ecdhe_rsa_aes_256_gcm_sha384** | **exp_rsa_des_cbc_sha** | **exp_rsa_rc2_md5** | **exp_rsa_rc4_md5** | **rsa_3des_ede_cbc_sha** | **rsa_aes_128_cbc_sha** | **rsa_aes_128_cbc_sha256** | **rsa_aes_256_cbc_sha** | **rsa_aes_256_cbc_sha256** | **rsa_des_cbc_sha** | **rsa_rc4_128_md5** | **rsa_rc4_128_sha** }

undo prefer-cipher

In FIPS mode:

prefer-cipher { **ecdhe_ecdsa_aes_128_cbc_sha256** | **ecdhe_ecdsa_aes_128_gcm_sha256** | **ecdhe_ecdsa_aes_256_cbc_sha384** | **ecdhe_ecdsa_aes_256_gcm_sha384** | **ecdhe_rsa_aes_128_cbc_sha256** | **ecdhe_rsa_aes_128_gcm_sha256** | **ecdhe_rsa_aes_256_cbc_sha384** | **ecdhe_rsa_aes_256_gcm_sha384** | **rsa_aes_128_cbc_sha** | **rsa_aes_128_cbc_sha256** | **rsa_aes_256_cbc_sha** | **rsa_aes_256_cbc_sha256** }

undo prefer-cipher

Default

In non-FIPS mode:

The preferred cipher suite of an SSL client policy is **rsa_rc4_128_md5**.

In FIPS mode:

The preferred cipher suite of an SSL client policy is **rsa_aes_128_cbc_sha**.

Views

SSL client policy view

Predefined user roles

network-admin

Parameters

dhe_rsa_aes_128_cbc_sha: Specifies the cipher suite that uses key exchange algorithm DHE RSA, data encryption algorithm 128-bit AES_CBC, and MAC algorithm SHA.

dhe_rsa_aes_128_cbc_sha256: Specifies the cipher suite that uses key exchange algorithm DHE RSA, data encryption algorithm 128-bit AES_CBC, and MAC algorithm SHA256.

dhe_rsa_aes_256_cbc_sha: Specifies the cipher suite that uses key exchange algorithm DHE RSA, data encryption algorithm 256-bit AES_CBC, and MAC algorithm SHA.

dhe_rsa_aes_256_cbc_sha256: Specifies the cipher suite that uses key exchange algorithm DHE RSA, data encryption algorithm 256-bit AES_CBC, and MAC algorithm SHA256.

ecdhe_ecdsa_aes_128_cbc_sha256: Specifies the cipher suite that uses key exchange algorithm ECDHE ECDSA, data encryption algorithm 128-bit AES_CBC, and MAC algorithm SHA256.

ecdhe_ecdsa_aes_128_gcm_sha256: Specifies the cipher suite that uses key exchange algorithm ECDHE ECDSA, data encryption algorithm 128-bit AES_GCM, and MAC algorithm SHA256.

ecdhe_ecdsa_aes_256_cbc_sha384: Specifies the cipher suite that uses key exchange algorithm ECDHE ECDSA, data encryption algorithm 256-bit AES_CBC, and MAC algorithm SHA384.

ecdhe_ecdsa_aes_256_gcm_sha384: Specifies the cipher suite that uses key exchange algorithm ECDHE ECDSA, data encryption algorithm 256-bit AES_GCM, and MAC algorithm SHA384.

ecdhe_rsa_aes_128_cbc_sha256: Specifies the cipher suite that uses key exchange algorithm ECDHE RSA, data encryption algorithm 128-bit AES_CBC, and MAC algorithm SHA256.

ecdhe_rsa_aes_128_gcm_sha256: Specifies the cipher suite that uses key exchange algorithm ECDHE RSA, data encryption algorithm 128-bit AES_GCM, and MAC algorithm SHA256.

ecdhe_rsa_aes_256_cbc_sha384: Specifies the cipher suite that uses key exchange algorithm ECDHE RSA, data encryption algorithm 256-bit AES_CBC, and MAC algorithm SHA384.

ecdhe_rsa_aes_256_gcm_sha384: Specifies the cipher suite that uses key exchange algorithm ECDHE RSA, data encryption algorithm 256-bit AES_GCM, and MAC algorithm SHA384.

exp_rsa_des_cbc_sha: Specifies the export cipher suite that uses key exchange algorithm RSA, data encryption algorithm DES_CBC, and MAC algorithm SHA.

exp_rsa_rc2_md5: Specifies the export cipher suite that uses key exchange algorithm RSA, data encryption algorithm RC2, and MAC algorithm MD5.

exp_rsa_rc4_md5: Specifies the export cipher suite that uses key exchange algorithm RSA, data encryption algorithm RC4, and MAC algorithm MD5.

rsa_3des_ede_cbc_sha: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm 3DES_EDE_CBC, and MAC algorithm SHA.

rsa_aes_128_cbc_sha: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm 128-bit AES_CBC, and MAC algorithm SHA.

rsa_aes_128_cbc_ sha256: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm 128-bit AES_CBC, and MAC algorithm SHA256.

rsa_aes_256_cbc_sha: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm 256-bit AES_CBC, and MAC algorithm SHA.

rsa_aes_256_cbc_ sha256: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm 256-bit AES_CBC, and MAC algorithm SHA256.

rsa_des_cbc_sha: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm DES_CBC, and MAC algorithm SHA.

rsa_rc4_128_md5: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm 128-bit RC4, and MAC algorithm MD5.

rsa_rc4_128_sha: Specifies the cipher suite that uses key exchange algorithm RSA, data encryption algorithm 128-bit RC4, and MAC algorithm SHA.

Usage guidelines

SSL employs the following algorithms:

- **Data encryption algorithms**—Encrypt data to ensure privacy. Commonly used data encryption algorithms are usually symmetric key algorithms. When using a symmetric key algorithm, the SSL server and the SSL client must use the same key.
- **Message Authentication Code (MAC) algorithms**—Calculate the MAC value for data to ensure integrity. Commonly used MAC algorithms include MD5 and SHA. When using a MAC algorithm, the SSL server and the SSL client must use the same key.
- **Key exchange algorithms**—Implement secure exchange of the keys used by the symmetric key algorithm and MAC algorithm. Commonly used key exchange algorithms are asymmetric key algorithms, such as RSA.

The SSL client sends the preferred cipher suite to the SSL server. The server compares the received cipher suite with the cipher suits it supports. If a match is found, the cipher suite negotiation succeeds. If no match is found, the negotiation fails.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure SSL client policy **policy1** to support the key exchange algorithm RSA, data encryption algorithm 128-bit AES_CBC, and MAC algorithm SHA.

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1] prefer-cipher rsa_aes_128_cbc_sha
```

Related commands

ciphersuite

display ssl client-policy

server-verify enable

Use **server-verify enable** to enable the SSL client to use digital certificates to authenticate the SSL server.

Use **undo server-verify enable** to disable SSL server authentication. The SSL client does not authenticate the SSL server.

Syntax

server-verify enable

undo server-verify enable

Default

The SSL client uses digital certificates to authenticate the SSL server.

Views

SSL client policy view

Predefined user roles

network-admin

Usage guidelines

SSL uses digital certificates to authenticate communicating parties. For more information about digital certificates, see *Security Configuration Guide*.

If you execute the **server-verify enable** command, the SSL server must send its digital certificate to the SSL client for authentication. The client can access the SSL server only after the server passes the authentication.

Examples

Enable the SSL client to use digital certificates to authenticate the SSL server.

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1] server-verify enable
```

Related commands

display ssl client-policy

session

Use **session** to set the maximum number of sessions that the SSL server can cache and the timeout time for cached sessions.

Use **undo session** to restore the default.

Syntax

session { **cachesize** *size* | **timeout** *time* } *

undo session { **cachesize** | **timeout** } *

Default

The SSL server can cache a maximum of 500 sessions, and the timeout time for cached sessions is 3600 seconds.

Views

SSL server policy view

Predefined user roles

network-admin

Parameters

cachesize *size*: Sets the maximum number of cached sessions, in the range of 100 to 20480.

timeout *time*: Sets the session cache timeout in the range of 1 to 4294967295 seconds.

Usage guidelines

The SSL server caches SSL sessions to reuse negotiated session parameters to simplify SSL handshake. Use this command to limit the maximum number and timeout time for cached sessions.

When the number of cached sessions reaches the maximum, SSL does not cache new sessions. When the timeout timer for a cached session expires, SSL deletes the session.

Examples

Set the maximum number of cached sessions to 600, and the timeout time for cached sessions to 1800 seconds.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] session cachesize 600 timeout 1800
```

Related commands

display ssl server-policy

ssl client-policy

Use **ssl client-policy** to create an SSL client policy and enter its view, or enter the view of an existing SSL client policy.

Use **undo ssl client-policy** to delete an SSL client policy.

Syntax

ssl client-policy *policy-name*

undo ssl client-policy *policy-name*

Default

No SSL client policies exist.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies an SSL client policy by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

This command creates an SSL client policy for which you can configure SSL parameters that the client uses to establish a connection to the server. The parameters include a PKI domain and a preferred cipher suite. An SSL client policy takes effect only after it is associated with an application.

Examples

Create an SSL client policy named **policy1** and enter its view.

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1]
```

Related commands

display ssl client-policy

ssl renegotiation disable

Use **ssl renegotiation disable** to disable SSL session renegotiation.

Use **undo ssl renegotiation disable** to restore the default.

Syntax

ssl renegotiation disable

undo ssl renegotiation disable

Default

SSL session renegotiation is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The SSL session renegotiation feature enables the SSL client and server to reuse a previously negotiated SSL session for an abbreviated handshake.

Disabling session renegotiation causes more computational overhead to the system but it can avoid potential risks. Disable SSL session renegotiation only when explicitly required.

Examples

#Disable SSL session renegotiation.

```
<Sysname> system-view
[Sysname] ssl renegotiation disable
```

ssl server-policy

Use **ssl server-policy** to create an SSL server policy and enter its view, or enter the view of an existing SSL server policy.

Use **undo ssl server-policy** to delete an SSL server policy.

Syntax

ssl server-policy *policy-name*

undo ssl server-policy *policy-name*

Default

No SSL server policies exist.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a name for the SSL server policy, a case-insensitive string of 1 to 31 characters.

Usage guidelines

This command creates an SSL server policy for which you can configure SSL parameters such as a PKI domain and supported cipher suits. An SSL server policy takes effect only after it is associated with an application such as HTTPS.

Examples

Create an SSL server policy named **policy1** and enter its view.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1]
```

Related commands

display ssl server-policy

ssl version disable

Use **ssl version disable** to disable the SSL server from using specific SSL protocol versions for session negotiation.

Use **undo ssl version disable** restore the default.

Syntax

In non-FIPS mode:

ssl version { **ssl3.0** | **tls1.0** | **tls1.1** } * **disable**

undo ssl version { **ssl3.0** | **tls1.0** | **tls1.1** } * **disable**

In FIPS mode:

ssl version { **tls1.0** | **tls1.1** } * **disable**

undo ssl version { **tls1.0** | **tls1.1** } * **disable**

Default

In non-FIPS mode:

The SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, and TLS 1.2.

In FIPS mode:

The SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2.

Views

System view

Predefined user roles

network-admin

Parameters

ssl3.0: Specifies SSL 3.0.

tls1.0: Specifies TLS 1.0.

tls1.1: Specifies TLS 1.1.

Usage guidelines

To enhance system security, you can disable the SSL server from using specific SSL protocol versions (SSL 3.0, TLS 1.0, and TLS 1.1) for session negotiation.

Disabling an SSL protocol version does not affect the availability of earlier SSL protocol versions. For example, if you execute the **ssl version tls1.1 disable** command, TLS 1.1 is disabled but TLS 1.0 is still available for the SSL server.

Examples

Disable SSL 3.0 for the SSL server.

```
<Sysname> system-view
[Sysname] ssl version ssl3.0 disable
```

version

Use **version** to specify an SSL protocol version for an SSL client policy.

Use **undo version** to restore the default.

Syntax

In non-FIPS mode:

version { **ssl3.0** | **tls1.0** | **tls1.1** | **tls1.2** }

undo version

In FIPS mode:

version { **tls1.0** | **tls1.1** | **tls1.2** }

undo version

Default

An SSL client policy uses SSL protocol version TLS 1.0.

Views

SSL client policy view

Predefined user roles

network-admin

Parameters

ssl3.0: Specifies SSL 3.0.

tls1.0: Specifies TLS 1.0.

tls1.1: Specifies TLS 1.1.

tls1.2: Specifies TLS 1.2.

Usage guidelines

To ensure security, do not specify SSL 3.0 for an SSL client policy.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the SSL protocol version to TLS 1.0 for SSL client policy **policy1**.

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1] version tls1.0
```

Related commands

display ssl client-policy

Contents

Attack detection and prevention commands

attack-defense login reauthentication-delay

Use **attack-defense login reauthentication-delay** to enable the login delay feature.

Use **undo attack-defense login reauthentication-delay** to restore the default.

Syntax

attack-defense login reauthentication-delay *seconds*

undo attack-defense login reauthentication-delay

Default

The login delay feature is disabled. The device does not delay accepting a login request from a user who has failed a login attempt.

Views

System view

Predefined user roles

network-admin

Parameters

seconds: Specifies the delay period in the range of 4 to 60 seconds.

Usage guidelines

The login delay feature delays the device to accept a login request from a user after the user fails a login attempt. This feature can slow down login dictionary attacks.

The login delay feature is independent of the login attack prevention feature.

Examples

Enable the login delay feature and set the delay period to 5 seconds.

```
<Sysname> system-view
[Sysname] attack-defense login reauthentication-delay 5
```

attack-defense tcp fragment enable

Use **attack-defense tcp fragment enable** to enable TCP fragment attack prevention.

Use **undo attack-defense tcp fragment enable** to disable TCP fragment attack prevention.

Syntax

attack-defense tcp fragment enable

undo attack-defense tcp fragment enable

Default

TCP fragment attack prevention is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command enables the device to drop attack TCP fragments to prevent TCP fragment attacks that the packet filter cannot detect. As defined in RFC 1858, attack TCP fragments refer to the following TCP fragments:

- First fragments in which the TCP header is smaller than 20 bytes.
- Non-first fragments with a fragment offset of 8 bytes (FO=1).

TCP fragment attack prevention takes precedence over single-packet attack prevention. When both are used, incoming TCP packets are processed first by TCP fragment attack prevention and then by the single-packet attack defense policy.

Examples

Enable TCP fragment attack prevention.

```
<Sysname> System-view
[Sysname] attack-defense tcp fragment enable
```

Contents

TCP attack prevention commands

tcp anti-naptha enable

Use **tcp anti-naptha enable** to enable Naptha attack prevention.

Use **undo tcp anti-naptha enable** to disable Naptha attack prevention.

Syntax

tcp anti-naptha enable

undo tcp anti-naptha enable

Default

Naptha attack prevention is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

After you enable Naptha attack prevention, the device periodically checks the number of TCP connections in each state. If the number of TCP connections in a state exceeds the limit, the device will accelerate the aging of the TCP connections in that state. The check interval is set by the **tcp check-state interval** command. The TCP connection limits are set by the **tcp state** command.

Examples

Enable Naptha attack prevention.

```
<Sysname> system-view
[Sysname] tcp anti-naptha enable
```

Related commands

tcp state

tcp check-state interval

tcp check-state interval

Use **tcp check-state interval** to set the interval for checking the number of TCP connections in each state.

Use **undo tcp check-state interval** to restore the default.

Syntax

tcp check-state interval *interval*

undo tcp check-state interval

Default

The interval for checking the number of TCP connections in each state is 30 seconds.

Views

System

Predefined user roles

network-admin

Parameter

interval: Specifies the check interval in the range of 1 to 60 seconds.

Usage guidelines

This command takes effect after you enable Naptha attack prevention.

After you enable Naptha attack prevention, the device checks the number of TCP connections in each state at intervals. If the number of TCP connections in a state exceeds the limit, the device will accelerate the aging of the TCP connections in that state.

Examples

Set the interval to 40 seconds for checking the number of TCP connections in each state.

```
<Sysname> system-view
[Sysname] tcp check-state interval 40
```

Related commands

tcp anti-naptha enable

tcp state

tcp state

Use **tcp state** to set the maximum number of TCP connections in a state.

Use **undo tcp state** to restore the default.

Syntax

tcp state { **closing** | **established** | **fin-wait-1** | **fin-wait-2** | **last-ack** } **connection-limit** *number*

undo tcp state { **closing** | **established** | **fin-wait-1** | **fin-wait-2** | **last-ack** } **connection-limit**

Default

The maximum number of TCP connections in each state (CLOSING, ESTABLISHED, FIN_WAIT_1, FIN_WAIT_2, and LAST_ACK) is 50.

Views

System view

Predefined user roles

network-admin

Parameters

closing: Specifies the CLOSING state.

established: Specifies the ESTABLISHED state.

fin-wait-1: Specifies the FIN_WAIT_1 state.

fin-wait-2: Specifies the FIN_WAIT_2 state.

last-ack: Specifies the LAST_ACK state.

connection-limit *number*: Specifies the maximum number of TCP connections, in the range of 0 to 500. The value of 0 represents that the device does not accelerate the aging of the TCP connections in a state.

Usage guidelines

This command takes effect after you enable Naptha attack prevention. If the number of TCP connections in a state exceeds the limit, the device will accelerate the aging of the TCP connections in the state.

Examples

Set the maximum number of TCP connections in the ESTABLISHED state to 100.

```
<Sysname> system-view
[Sysname] tcp state established connection-limit 100
```

Related commands

tcp anti-naptha enable

tcp check-state interval

Contents

IP source guard commands

display ip source binding

Use **display ip source binding** to display IPv4SG bindings.

Syntax

display ip source binding [**static** | [**arp-snooping-vlan** | **dhcp-relay** | **dhcp-server** | **dhcp-snooping** | **dot1x**]] [**ip-address** *ip-address*] [**mac-address** *mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

static: Displays static IPv4SG bindings.

arp-snooping-vlan: Specifies IPv4SG bindings generated based on ARP snooping for VLANs.

dhcp-relay: Specifies IPv4SG bindings generated based on DHCP relay agent.

dhcp-server: Specifies IPv4SG bindings generated based on DHCP server.

dhcp-snooping: Specifies IPv4SG bindings generated based on DHCP snooping.

dot1x: Specifies IPv4SG bindings generated based on 802.1X. To display dynamic IPv4SG bindings generated based on the 802.1X module, you must also specify the slot through which 802.1X users access the network.

ip-address *ip-address*: Specifies an IPv4 address.

mac-address *mac-address*: Specifies a MAC address in H-H-H format.

vlan *vlan-id*: Specifies a VLAN ID in the range of 1 to 4094.

interface *interface-type interface-number*: Specifies an interface by its type and number.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv4SG bindings for the master device.

Examples

Display all IPSG bindings on the public network.

```
<Sysname> display ip source binding
Total entries found: 5
IP Address      MAC Address    Interface               VLAN Type
10.1.0.5        040a-0000-4000 GE1/0/1                 1    DHCP snooping
10.1.0.6        040a-0000-3000 GE1/0/1                 1    DHCP snooping
10.1.0.7        040a-0000-2000 GE1/0/1                 1    DHCP snooping
10.1.0.8        040a-0000-1000 GE1/0/2                 N/A  DHCP relay
10.1.0.9        040a-0000-2000 GE1/0/2                 N/A  Static
```

Table 1 Command output

Field	Description
Total entries found	Total number of IPv4SG bindings.
IP Address	IPv4 address in the IPv4SG binding. If no IP address is bound in the binding, this field displays **N/A**.
MAC Address	MAC address in the IPv4SG binding. If no MAC address is bound in the binding, this field displays **N/A**.
Interface	Interface of the binding. This field displays **N/A** for a global IPv4SG binding.
VLAN	VLAN information in the IPv4SG binding. If the binding contains no VLAN information, this field displays **N/A**.
Type	IPSG binding type: • **Static**—Manually configured by using the **ip source binding** command. Static bindings are for packet filtering in IPSG or used by other modules to provide security services. • **ARP snooping vlan**—Dynamically generated based on ARP snooping for the VLAN. The binding is for packet filtering in IPSG. • **802.1X**—Dynamically generated based on 802.1X. The binding is for packet filtering in IPSG. • **DHCP relay**—Dynamically generated based on DHCP relay agent. The binding is for packet filtering in IPSG. • **DHCP server**—Dynamically generated based on DHCP server. The binding is used by other modules to provide security services. • **DHCP snooping**—Dynamically generated based on DHCP snooping. The binding is for packet filtering in IPSG.

Related commands

ip source binding

ip verify source

display ip verify source excluded

Use **display ip verify source excluded** to display source items that have been configured to be excluded from IPSG filtering.

Syntax

display ip verify source excluded [**vlan** *start-vlan-id* [**to** *end-vlan-id*]] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan *start-vlan-id* [**to** *end-vlan-id*]: Specifies VLANs that have been configured to be excluded from IPSG filtering. Value ranges for both the *start-vlan-id* and *end-vlan-id* arguments are 1 to 4094. The value for the *end-vlan-id* argument must be equal to or greater than the value for the *start-vlan-id* argument.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices.

Examples

Display all source items that have been configured to be excluded from IPSG filtering.

```
<Sysname> display ip verify source excluded
Slot:
  Start VLAN ID        End VLAN ID    Status
  1                    20             Active
  24                   50             Active
  200                  300            Inactive
```

Display VLANs (VLAN 3 and VLAN 5 through VLAN 10) that have been configured to be excluded from IPSG filtering.

```
<Sysname> display ip verify source excluded vlan 3
Slot:
  VLAN ID: 3
  Status: Active

<Sysname> display ip verify source excluded vlan 5 to 10
Slot:
  Start VLAN ID        End VLAN ID    Status
  5                    10             Active
```

Table 2 Command output

Field	Description
Start VLAN ID	Start VLAN ID of the VLAN range that has been configured to be excluded from IPSG filtering.
End VLAN ID	End VLAN ID of the VLAN range that has been configured to be excluded from IPSG filtering.
Status	Whether the excluded VLAN configuration takes effect: • **Active**—The configuration takes effect. • **Inactive**—The configuration does not take effect.

Related commands

ip verify source exclude

display ipv6 source binding

Use **display ipv6 source binding** to display IPv6SG address bindings.

Syntax

display ipv6 source binding [**static** | [**dhcpv6-server** | **dhcpv6-snooping** | **dot1x**]] [**ip-address** *ipv6-address*] [**mac-address** *mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

`static`: Displays static IPv6SG address bindings.

`dhcpv6-server`: Specifies IPv6SG bindings generated based on DHCPv6 server.

`dhcpv6-snooping`: Specifies IPv6SG bindings generated based on DHCPv6 snooping.

`dot1x`: Specifies IPv6SG bindings generated based on 802.1X. To display dynamic IPv6SG address bindings generated based on the 802.1X module, you must also specify the slot through which 802.1X users access the network.

`ip-address` *`ipv6-address`*: Specifies an IPv6 address.

`mac-address` *`mac-address`*: Specifies a MAC address in H-H-H format.

`vlan` *`vlan-id`*: Specifies a VLAN ID in the range of 1 to 4094.

`interface` *`interface-type interface-number`*: Specifies an interface by its type and number.

`slot` *`slot-number`*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6SG address bindings for the master device.

Examples

Display all IPv6SG address bindings on the public network.

```
<Sysname> display ipv6 source binding
Total entries found: 2
IPv6 Address         MAC Address    Interface              VLAN Type
2012:1222:2012:1222: 000f-2202-0435 GE1/0/1                1    DHCPv6 snooping
2012:1222:2012:1222
2012:1222:2012:1222: 000f-2202-0436 GE1/0/1                N/A  Static
2012:1222:2012:1223
```

Table 3 Command output

Field	Description
Total entries found	Total number of IPv6SG address bindings.
IPv6 Address	IPv6 address in the IPv6SG address binding. If no IPv6 address is bound in the binding, this field displays **N/A**.
MAC Address	MAC address in the IPv6SG address binding. If no MAC address is bound in the binding, this field displays **N/A**.
Interface	Interface of the IPv6SG address binding. This field displays **N/A** for a global IPv6SG binding.
VLAN	VLAN information in the IPv6SG address binding. If the binding contains no VLAN information, this field displays **N/A**.

Field	Description
Type	Type of the IPv6SG address binding: • **Static**—Manually configured by using the **ipv6 source binding** command. Static bindings are for packet filtering in IPv6SG or used by other modules to provide security services. • **DHCPv6 sever**—Dynamically generated based on DHCPv6 server. The binding is reported to the controller for the controller to understand the information about online and offline users. The binding is not for packet filtering. • **DHCPv6 snooping**—Dynamically generated based on DHCPv6 snooping. The binding is for packet filtering in IPv6SG. • **802.1X**—Dynamically generated based on 802.1X. The binding is for packet filtering in IPv6SG.

Related commands

ipv6 source binding

ipv6 verify source

display ipv6 source binding pd

Use **display ipv6 source binding pd** to display IPv6SG prefix bindings.

Syntax

display ipv6 source binding pd [**prefix** *prefix/prefix-length*] [**mac-address** *mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**slot** *slot-number*]

Views

Any views

Predefined user roles

network-admin

network-operator

Parameters

prefix *prefix/prefix-length*: Specifies an IPv6 prefix. The value range for the *prefix-length* argument is 1 to 128. If you do not specify an IPv6 prefix, this command displays all IPv6SG prefix bindings.

mac-address *mac-address*: Specifies a MAC address in H-H-H format. If you do not specify a MAC address, this command displays IPv6SG prefix bindings for all MAC addresses.

vlan *vlan-id*: Specifies a VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays IPv6SG prefix bindings for all VLANs.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays IPv6SG prefix bindings for all interfaces.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6SG prefix bindings for the master device.

Usage guidelines

IPv6SG prefix bindings are dynamically obtained from the DHCPv6 snooping module.

Examples

Display all IPv6SG prefix bindings.

```
<Sysname> display ipv6 source binding pd
Total entries found: 3
IPv6 prefix          MAC address     Interface      VLAN  Type
2012:1111::/64       000f-2202-0435  GE1/0/1        1     DHCPv6 snooping
2012:2222::/64       000f-2202-0436  GE2/0/1        2     DHCPv6 snooping
```

Table 4 Command output

Field	Description
Total entries found	Total number of IPv6SG prefix bindings.
IPv6 prefix	IPv6 prefix and prefix length in the IPv6SG prefix binding.
MAC address	MAC address in the IPv6SG prefix binding. This field displays **N/A** if the MAC address is invalid.
Interface	Interface to which the IPv6SG prefix binding belongs. This field displays **N/A** for a global IPv6SG prefix binding or an IPv6SG prefix binding generated based on an ND RA prefix entry.
VLAN	VLAN information in the IPv6SG prefix binding. This field displays **N/A** if the IPv6SG prefix binding does not contain the VLAN information.
Type	Type of the IPv6SG prefix binding: **DHCPv6 snooping**—The binding is generated based on a DHCPv6 snooping entry.

Related commands

ipv6 source binding

ipv6 verify source

ip source binding (interface view)

Use **ip source binding** to configure a static IPv4SG binding on an interface.

Use **undo ip source binding** to delete the static IPv4SG bindings configured on an interface.

Syntax

ip source binding { **ip-address** *ip-address* | **ip-address** *ip-address* **mac-address** *mac-address* | **mac-address** *mac-address* } [**vlan** *vlan-id*]

undo ip source binding { **all** | **ip-address** *ip-address* | **ip-address** *ip-address* **mac-address** *mac-address* | **mac-address** *mac-address* } [**vlan** *vlan-id*]

Default

No static IPv4SG bindings exist on an interface.

Views

Layer 2 Ethernet interface view

VLAN interface view

Predefined user roles

network-admin

Parameters

all: Removes all static IPv4SG bindings on the interface.

ip-address *ip-address*: Specifies an IPv4 address for the static binding. The IPv4 address must be a class A, B, or C address, and cannot be 127.x.x.x or 0.0.0.0.

mac-address *mac-address*: Specifies a MAC address for the static binding. The MAC address must be in H-H-H format, and cannot be all 0s, all Fs (a broadcast MAC address), or a multicast MAC address.

vlan *vlan-id*: Specifies a VLAN ID for the static binding. The value range is 1 to 4094. This option is supported only in Layer 2 Ethernet interface view.

Usage guidelines

Static IPv4SG bindings on an interface implement the following functions:

- Filter incoming IPv4 packets on the interface.
- Check user validity by cooperating with the ARP attack detection feature.

Examples

Configure a static IPv4SG binding on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip source binding ip-address 192.168.0.1 mac-address
0001-0001-0001
```

Related commands

display ip source binding

ip source binding (system view)

ip source binding (system view)

Use **ip source binding** to configure a global static IPv4SG binding.

Use **undo ip source binding** to delete one or all global static IPv4SG bindings.

Syntax

ip source binding ip-address *ip-address* **mac-address** *mac-address*

undo ip source binding { **all** | **ip-address** *ip-address* **mac-address** *mac-address* }

Default

No global static IPv4SG bindings exist.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address *ip-address*: Specifies the IPv4 address for the static binding. The IPv4 address must be a class A, B, or C address, and cannot be 127.x.x.x or 0.0.0.0.

mac-address *mac-address*: Specifies the MAC address for the static binding. The MAC address is in the format H-H-H but cannot be all 0s, all Fs (a broadcast MAC address), or a multicast MAC address.

all: Removes all global static IPv4SG bindings.

Usage guidelines

A global static IPv4SG binding takes effect on all interfaces.

Examples

Configure a global static IPv4SG binding.

```
<Sysname> system-view
[Sysname] ip source binding ip-address 192.168.0.1 mac-address 0001-0001-0001
```

Related commands

display ip source binding

ip source binding (interface view)

ip verify source

Use **ip verify source** to enable IPv4SG on an interface.

Use **undo ip verify source** to disable IPv4SG on an interface.

Syntax

ip verify source { **ip-address** | **ip-address mac-address** | **mac-address** }

undo ip verify source

Default

The IPv4SG feature is disabled on an interface.

Views

Layer 2 Ethernet interface view

Layer 3 aggregate subinterface view

VLAN interface view

Predefined user roles

network-admin

Parameters

ip-address: Filters incoming packets by source IPv4 addresses.

ip-address mac-address: Filters incoming packets by source IPv4 addresses and source MAC addresses.

mac-address: Filters incoming packets by source MAC addresses.

Usage guidelines

After you enable IPv4SG on an interface, this feature uses static and dynamic IPv4SG bindings to match incoming packets on the interface. Packets that match an IPv4SG binding are forwarded and packets that do not match any IPv4SG binding are discarded.

The matching criterion specified by this command applies only to dynamic IPSG. Static IPv4SG uses static bindings configured by using the **ip source binding** command.

If you re-execute this command to modify the matching criterion, the new criterion applies only to packets of the access users that come online after the command execution.

You can configure IPv4SG on an interface multiple times, the most recent configuration takes effect.

Examples

Enable IPv4SG on Layer 2 Ethernet interface GigabitEthernet 1/0/1 and verify the source IPv4 address and MAC address for dynamic IPSG.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip verify source ip-address mac-address
```

Enable IPv4SG on VLAN-interface 100 and verify the source IPv4 address and MAC address for dynamic IPSG.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ip verify source ip-address mac-address
```

Related commands

display ip source binding

ip verify source exclude

Use **ip verify source exclude** to exclude IPv4 packets with the specified source items from IPSG filtering.

Use **undo ip verify source exclude** to remove the specified excluded source items.

Syntax

ip verify source exclude vlan *start-vlan-id* [**to** *end-vlan-id*]

undo ip verify source exclude vlan *start-vlan-id* [**to** *end-vlan-id*]

Default

No excluded source items are configured.

Views

System view

Predefined user roles

network-admin

Parameters

vlan *start-vlan-id* [**to** *end-vlan-id*]: Specifies excluded VLANs. Value ranges for both the *start-vlan-id* and *end-vlan-id* arguments are 1 to 4094. The value for the *end-vlan-id* argument must be equal to or greater than the value for the *start-vlan-id* argument. A single excluded VLAN is specified if you specify only the *start-vlan-id* argument or specify the same VLAN ID for the *start-vlan-id* and *end-vlan-id* arguments.

Usage guidelines

This command allows all IPv4 packets with the specified source items to be forwarded without being processed by IPSG.

You can execute this command multiple times to specify multiple excluded VLANs. The specified excluded VLANs cannot overlap.

To successfully delete excluded VLANs, make sure the VLANs specified in the **undo** form of this command are the same as the VLANs specified when you configure excluded VLANs.

Examples

Exclude IPv4 packets from VLAN 3 and VLAN 5 through VLAN 10 from IPSG filtering.

```
<Sysname> system-view
[Sysname] ip verify source exclude vlan 3
[Sysname] ip verify source exclude vlan 5 to 10
```

Related commands

display ip verify source excluded

ipv6 source binding (interface view)

Use **ipv6 source binding** to configure a static IPv6SG binding.

Use **undo ipv6 source binding** to delete the static IPv6SG bindings configured on an interface.

Syntax

ipv6 source binding { **ip-address** *ipv6-address* | **ip-address** *ipv6-address* **mac-address** *mac-address* | **mac-address** *mac-address* } [**vlan** *vlan-id*]

undo ipv6 source binding { **all** | **ip-address** *ipv6-address* | **ip-address** *ipv6-address* **mac-address** *mac-address* | **mac-address** *mac-address* } [**vlan** *vlan-id*]

Default

No static IPv6SG bindings exist on an interface.

Views

Layer 2 Ethernet interface view

Layer 3 aggregate subinterface view

VLAN interface view

Predefined user roles

network-admin

Parameters

all: Removes all the static IPv6SG bindings on the interface.

ip-address *ipv6-address*: Specifies an IPv6 address for the static binding. The IPv6 address cannot be an all-zero address, a multicast address, or a loopback address.

mac-address *mac-address*: Specifies a MAC address for the static binding. The MAC address must be in H-H-H format, and cannot be all 0s, all Fs (a broadcast MAC address), or a multicast MAC address.

vlan *vlan-id*: Specifies a VLAN ID for the static binding. The value range is 1 to 4094. This option is supported only in Layer 2 Ethernet interface view.

Usage guidelines

Static IPv6SG bindings on an interface filter incoming IPv6 packets.

Examples

Configure a static IPv6SG binding on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 source binding ip-address 2001::1 mac-address
0002-0002-0002
```

Related commands

display ipv6 source binding

display ipv6 source binding pd

ipv6 source binding (system view)

ipv6 source binding (system view)

Use **ipv6 source binding** to configure a global static IPv6SG binding.

Use **undo ipv6 source binding** to delete one or all global static IPv6SG bindings.

Syntax

ipv6 source binding ip-address *ipv6-address* **mac-address** *mac-address*

undo ipv6 source binding { **all** | **ip-address** *ipv6-address* **mac-address** *mac-address* }

Default

No global static IPv6SG bindings exist.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6-address *ipv6-address*: Specifies the IPv6 address for the static binding. The IPv6 address cannot be an all-zero address, a multicast address, or a loopback address.

mac-address *mac-address*: Specifies the MAC address for the static binding. The MAC address must be in H-H-H format, and cannot be all 0s, all Fs (a broadcast MAC address), or a multicast MAC address.

all: Removes all global static IPv6SG bindings.

Usage guidelines

A global static IPv6SG binding takes effect on all interfaces.

Examples

Configure a global static IPv6SG binding.

```
<Sysname> system-view
[Sysname] ipv6 source binding ipv6-address 2001::1 mac-address 0002-0002-0002
```

Related commands

display ipv6 source binding

display ipv6 source binding pd

ipv6 source binding (interface view)

ipv6 verify source

Use **ipv6 verify source** to enable IPv6SG on an interface.

Use **undo ipv6 verify source** to disable IPv6SG on an interface.

Syntax

ipv6 verify source { **ip-address** | **ip-address mac-address** | **mac-address** }

undo ipv6 verify source

Default

The IPv6SG feature is disabled on an interface.

Views

Layer 2 Ethernet interface view

Layer 3 aggregate subinterface view

VLAN interface view

Predefined user roles

network-admin

Parameters

ip-address: Filters incoming packets by source IPv6 addresses.

ip-address mac-address: Filters incoming packets by source IPv6 addresses and source MAC addresses.

mac-address: Filters incoming packets by source MAC addresses.

Usage guidelines

After you enable IPv6SG on an interface, this feature uses static and dynamic IPv6SG bindings to match incoming packets on the interface. Packets that match an IPv6SG binding are forwarded and packets that do not match any IPv6SG binding are discarded.

The matching criterion specified by this command applies only to dynamic IPv6SG. Static IPv6SG uses static bindings configured by using the **ipv6 source binding** command.

If you re-execute this command to modify the matching criterion, the new criterion applies only to packets of the access users that come online after the command execution.

You can configure IPv6SG on an interface multiple times, the most recent configuration takes effect.

Examples

Enable IPv6SG on Layer 2 Ethernet interface GigabitEthernet 1/0/1 and verify the source IPv6 address and MAC address for dynamic IPv6SG.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 verify source ip-address mac-address
```

Related commands

display ipv6 source binding

display ipv6 source binding pd

Contents

ARP attack protection commands

Unresolvable IP attack protection commands

arp resolving-route enable

Use **arp resolving-route enable** to enable ARP blackhole routing.

Use **undo arp resolving-route enable** to disable ARP blackhole routing.

Syntax

arp resolving-route enable

undo arp resolving-route enable

Default

ARP blackhole routing is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Configure this command on the gateways.

Examples

Enable ARP blackhole routing.

```
<Sysname> system-view
[Sysname] arp resolving-route enable
```

Related commands

arp resolving-route probe-count

arp resolving-route probe-interval

arp resolving-route probe-count

Use **arp resolving-route probe-count** to set the number of ARP blackhole route probes for each unresolved IP address.

Use **undo arp resolving-route probe-count** to restore the default.

Syntax

arp resolving-route probe-count *count*

undo arp resolving-route probe-count

Default

The device performs three ARP blackhole route probes for each unresolved IP address.

Views

System view

Predefined user roles

network-admin

Parameters

count: Sets the number of probes, in the range of 1 to 25.

Examples

Configure the device to perform five ARP blackhole route probes for each unresolved IP address.

```
<Sysname> system-view
[Sysname] arp resolving-route probe-count 5
```

Related commands

arp resolving-route enable

arp resolving-route probe-interval

arp resolving-route probe-interval

Use **arp resolving-route probe-interval** to set the interval at which the device probes ARP blackhole routes.

Use **undo arp resolving-route probe-interval** to restore the default.

Syntax

arp resolving-route probe-interval *interval*

undo arp resolving-route probe-interval

Default

The device probes ARP blackhole routes every 1 second.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the probe interval in the range of 1 to 5 seconds.

Examples

Configure the device to probe ARP blackhole routes every 3 seconds.

```
<Sysname> system-view
[Sysname] arp resolving-route probe-interval 3
```

Related commands

arp resolving-route enable

arp resolving-route probe-count

arp source-suppression enable

Use **arp source-suppression enable** to enable the ARP source suppression feature.

Use **undo arp source-suppression enable** to disable the ARP source suppression feature.

Syntax

arp source-suppression enable

undo arp source-suppression enable

Default

The ARP source suppression feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Configure this feature on the gateways.

Examples

Enable the ARP source suppression feature.

```
<Sysname> system-view
[Sysname] arp source-suppression enable
```

Related commands

display arp source-suppression

arp source-suppression limit

Use **arp source-suppression limit** to set the maximum number of unresolvable packets that can be processed per source IP address within 5 seconds.

Use **undo arp source-suppression limit** to restore the default.

Syntax

arp source-suppression limit *limit-value*

undo arp source-suppression limit

Default

The device can process a maximum of 10 unresolvable packets per source IP address within 5 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

limit-value: Specifies the limit in the range of 2 to 1024.

Usage guidelines

If unresolvable packets received from an IP address within 5 seconds exceed the limit, the device stops processing the packets from that IP address until the 5 seconds elapse.

Examples

Configure the device to process a maximum of 100 unresolvable packets per source IP address within 5 seconds.

```
<Sysname> system-view
[Sysname] arp source-suppression limit 100
```

Related commands

display arp source-suppression

display arp source-suppression

Use **display arp source-suppression** to display information about the current ARP source suppression configuration.

Syntax

display arp source-suppression

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display information about the current ARP source suppression configuration.

```
<Sysname> display arp source-suppression
 ARP source suppression is enabled
 Current suppression limit: 100
```

Table 1 Command output

Field	Description
Current suppression limit	Maximum number of unresolvable packets that can be processed per source IP address within 5 seconds.

ARP packet rate limit commands

arp rate-limit

Use **arp rate-limit** to enable the ARP packet rate limit feature on an interface.

Use **undo arp rate-limit** to disable the ARP packet rate limit feature on an interface.

Syntax

arp rate-limit [*pps*]

undo arp rate-limit

Default

The ARP packet rate limit feature is enabled on an interface.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

pps: Specifies the upper limit for ARP packet rate in pps. The value range for this argument is 5 to 200.

Usage guidelines

If you do not specify a value for the *pps* argument in the **arp rate-limit** command, the default rate limit value applies. Packets that exceed the rate limit are discarded.

Examples

Enable the ARP packet rate limit feature on GigabitEthernet 1/0/1, and set the maximum ARP packet rate to 50 pps.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp rate-limit 50
```

arp rate-limit log enable

Use **arp rate-limit log enable** to enable logging for ARP packet rate limit.

Use **undo arp rate-limit log enable** to disable logging for ARP packet rate limit.

Syntax

arp rate-limit log enable

undo arp rate-limit log enable

Default

Logging for ARP packet rate limit is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

When logging for ARP packet rate limit is enabled, the device sends the highest threshold-crossed ARP packet rate within the sending interval in a log message to the information center. You can configure the information center module to set the log output rules. For more information about information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Enable logging for ARP packet rate limit.

```
<Sysname> system-view
[Sysname] arp rate-limit log enable
```

arp rate-limit log interval

Use **arp rate-limit log interval** to set the notification and log message sending interval for ARP packet rate limit.

Use **undo arp rate-limit log interval** to restore the default.

Syntax

arp rate-limit log interval *interval*

undo arp rate-limit log interval

Default

The device sends notifications or log messages every 60 seconds when the rate of ARP packets received on an interface exceeds the limit.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies an interval in the range of 1 to 86400 seconds.

Usage guidelines

To change the default interval and activate it, you must enable ARP packet rate limit and enable sending notifications or log messages for ARP packet rate limit.

Examples

Set the device to send notifications and log messages every 120 seconds when the rate of ARP packets received on an interface exceeds the limit.

```
<Sysname> system-view
[Sysname] arp rate-limit log interval 120
```

Related commands

arp rate-limit

arp rate-limit log enable

snmp-agent trap enable arp

snmp-agent trap enable arp

Use **snmp-agent trap enable arp** to enable SNMP notifications for ARP.

Use **undo snmp-agent trap enable arp** to disable SNMP notifications for ARP.

Syntax

snmp-agent trap enable arp [**rate-limit**]

undo snmp-agent trap enable arp [**rate-limit**]

Default

SNMP notifications for ARP is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

rate-limit: Specifies the ARP packet rate limit feature.

Usage guidelines

After you enable SNMP notifications for ARP, the device generates a notification that includes the highest threshold-crossed ARP packet rate within the sending interval.

For ARP event notifications to be sent correctly, you must also configure SNMP on the device. For more information about SNMP configuration, see the network management and monitoring configuration guide for the device.

Examples

Enable SNMP notifications for ARP packet rate limit.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable arp rate-limit
```

Source MAC-based ARP attack detection commands

arp source-mac

Use **arp source-mac** to enable the source MAC-based ARP attack detection feature and specify a handling method.

Use **undo arp source-mac** to disable the source MAC-based ARP attack detection feature.

Syntax

arp source-mac { **filter** | **monitor** }

undo arp source-mac [**filter** | **monitor**]

Default

The source MAC-based ARP attack detection feature is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

filter: Specifies the filter handling method.

monitor: Specifies the monitor handling method.

Usage guidelines

Configure this feature on the gateways.

This feature checks the number of ARP packets delivered to the CPU. If the number of packets from the same MAC address within 5 seconds exceeds a threshold, the device generates an ARP attack entry for the MAC address. Before the entry ages out, the device handles the attack by using either of the following methods:

- **Monitor**—Only generates log messages.
- **Filter**—Generates log messages and filters out subsequent ARP packets from the MAC address and data packets sources from or destined for the MAC address.

Make sure you have enabled the ARP logging feature before enabling the source MAC-based ARP attack detection feature. For information about the ARP logging feature, see *Layer 3—IP Services Configuration Guide*.

If you do not specify any handling method in the **undo arp source-mac** command, the command disables this feature.

Examples

Enable the source MAC-based ARP attack detection feature and specify the filter handling method.

```
<Sysname> system-view
[Sysname] arp source-mac filter
```

arp source-mac aging-time

Use **arp source-mac aging-time** to set the aging time for ARP attack entries.

Use **undo arp source-mac aging-time** to restore the default.

Syntax

arp source-mac aging-time *time*

undo arp source-mac aging-time

Default

The aging time for ARP attack entries is 300 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

time: Sets the aging time for ARP attack entries, in the range of 60 to 6000 seconds.

Examples

Set the aging time for ARP attack entries to 60 seconds.

```
<Sysname> system-view
[Sysname] arp source-mac aging-time 60
```

arp source-mac exclude-mac

Use **arp source-mac exclude-mac** to exclude specific MAC addresses from source MAC-based ARP attack detection.

Use **undo arp source-mac exclude-mac** to remove the excluded MAC addresses from source MAC-based ARP attack detection.

Syntax

arp source-mac exclude-mac *mac-address*&<1-10>

undo arp source-mac exclude-mac [*mac-address*&<1-10>]

Default

No MAC addresses are excluded from source MAC-based ARP attack detection.

Views

System view

Predefined user roles

network-admin

Parameters

mac-address&<1-10>: Specifies a MAC address list. The *mac-address* argument indicates an excluded MAC address in the format of H-H-H. &<1-10> indicates that you can specify a maximum of 10 excluded MAC addresses each time.

Usage guidelines

If you do not specify a MAC address, the **undo arp source-mac exclude-mac** command removes all excluded MAC addresses.

You can repeat this command to configure a maximum of 64 MAC addresses excluded from source MAC-based ARP attack detection.

Examples

Exclude a MAC address from source MAC-based ARP attack detection.

```
<Sysname> system-view
[Sysname] arp source-mac exclude-mac 001e-1200-0213
```

arp source-mac log enable

Use **arp source-mac log enable** to enable logging for source MAC-based ARP attack detection.

Use **undo arp source-mac log enable** to disable logging for source MAC-based ARP attack detection.

Syntax

arp source-mac log enable

undo arp source-mac log enable

Default

Logging for source MAC-based ARP attack detection is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

When the device detects a source MAC-based ARP attack, it generates a log message and sends it to the information center. For information about the log destination and output rule configuration in the information center, see *Network Management and Monitoring Configuration Guide*.

The log messages help administrators to locate and solve problems.

Examples

Enable logging for source MAC-based ARP attack detection.

```
<Sysname> system-view
[Sysname] arp source-mac log enable
```

arp source-mac threshold

Use **arp source-mac threshold** to set the threshold for source MAC-based ARP attack detection. If the number of ARP packets sent from a MAC address within 5 seconds exceeds this threshold, the device recognizes this as an attack.

Use **undo arp source-mac threshold** to restore the default.

Syntax

arp source-mac threshold *threshold-value*

undo arp source-mac threshold

Default

The threshold for source MAC-based ARP attack detection is 30.

Views

System view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the threshold for source MAC-based ARP attack detection. The value range for this argument is 1 to 5000.

Examples

Set the threshold for source MAC-based ARP attack detection to 30.

```
<Sysname> system-view
[Sysname] arp source-mac threshold 30
```

display arp source-mac

Use **display arp source-mac** to display ARP attack entries detected by source MAC-based ARP attack detection.

Syntax

display arp source-mac { **interface** *interface-type interface-number* [**slot** *slot-number*] | **slot** *slot-number* }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

slot *slot-number*: Displays the ARP attack entries detected by the physical interfaces that reside on the specified member device and belong to the virtual interface. If you do not specify a member device, this command displays entries detected by the physical interfaces that reside on the master device and belong to the specified virtual interface.

slot *slot-number*: Specifies an IRF member device by its ID. If you do not specify a member device, this command displays ARP attack entries for the master device.

Usage guidelines

The **slot** *slot-number* option is supported only when the **interface** *interface-type interface-number* option specifies a virtual interface.

Virtual interfaces can be only Layer 2 aggregate interfaces.

Examples

Display the ARP attack entries detected by source MAC-based ARP attack detection on GigabitEthernet 1/0/1.

```
<Sysname> display arp source-mac interface gigabitethernet 1/0/1
Source-MAC       VLAN/VSI name     Interface               Aging-time (sec)
23f3-1122-3344   4094              GE1/0/1                 10
```

Table 2 Command output

Field	Description
Source-MAC	Source MAC address of the attack.
VLAN ID/VSI name	This field is not supported in the current software version. ID of the VLAN or name of the name of the VSI in which the attack was detected. If the detected attack does not belong to any VLAN or VSI, this field displays **N/A**.
Interface	Interface on which the attack was detected.
Aging-time (sec)	Aging time for the ARP attack entry, in seconds.

ARP packet source MAC consistency check commands

arp valid-check enable

Use **arp valid-check enable** to enable ARP packet source MAC address consistency check.

Use **undo arp valid-check enable** to disable ARP packet source MAC address consistency check.

Syntax

arp valid-check enable

undo arp valid-check enable

Default

ARP packet source MAC address consistency check is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Configure this feature on gateways. The gateways can filter out ARP packets whose source MAC address in the Ethernet header is different from the sender MAC address in the message body.

Examples

Enable ARP packet source MAC address consistency check.

```
<Sysname> system-view
[Sysname] arp valid-check enable
```

ARP active acknowledgement commands

arp active-ack enable

Use **arp active-ack enable** to enable the ARP active acknowledgement feature.

Use **undo arp active-ack enable** to disable the ARP active acknowledgement feature.

Syntax

arp active-ack [**strict**] **enable**

undo arp active-ack [**strict**] **enable**

Default

The ARP active acknowledgement feature is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

strict: Enables strict mode for ARP active acknowledgement.

Usage guidelines

Configure this feature on gateways to prevent user spoofing.

In strict mode, a gateway learns an entry only when ARP active acknowledgement is successful based on the correct ARP resolution.

Examples

Enable the ARP active acknowledgement feature.

```
<Sysname> system-view
[Sysname] arp active-ack enable
```

Authorized ARP commands

arp authorized enable

Use **arp authorized enable** to enable authorized ARP on an interface.

Use **undo arp authorized enable** to disable authorized ARP on an interface.

Syntax

arp authorized enable

undo arp authorized enable

Default

Authorized ARP is disabled on the interface.

Views

VLAN interface view

Predefined user roles

network-admin

Examples

Enable authorized ARP on VLAN-interface 200.

```
<Sysname> system-view
[Sysname] interface vlan-interface 200
[Sysname-Vlan-interface200] arp authorized enable
```

ARP attack detection commands

arp detection enable

Use **arp detection enable** to enable ARP attack detection.

Use **undo arp detection enable** to disable ARP attack detection.

Syntax

arp detection enable

undo arp detection enable

Default

ARP attack detection is disabled.

Views

VLAN view

Predefined user roles

network-admin

Examples

Enable ARP attack detection for VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] arp detection enable
```

Related commands

arp detection rule

display arp detection

display arp detection statistics attack-source

reset arp detection statistics attack-source

arp detection log enable

Use **arp detection log enable** to enable ARP attack detection logging.

Use **undo arp detection log enable** to disable ARP attack detection logging.

Syntax

arp detection log enable [**interval** *interval* | **number** *number*]

undo arp detection log enable

Default

ARP attack detection logging is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

interval *interval*: Specifies the interval for sending ARP attack detection logs to the information center, in seconds. The value for this argument can be 0 or a value in the range of 10 to 3600. The default value is 60. If you set the interval to 0 seconds, the device sends ARP detection logs to the information center immediately.

number *number*: Specifies the maximum number of ARP attack detection logs for each log output. The value range for the *number* argument is 1 to 128, and the default value is 128.

Usage guidelines

This feature enables the device to generate ARP detection logs and send them to the information center. For information about the log destination and output rule configuration in the information center, see *Network Management and Monitoring Configuration Guide*.

As a best practice, disable this feature if the log generation affects the device performance.

Excessive number of logs not only affects the device performance, but also makes it difficult for you to locate logs for specific events. To resolve the issue, you can adjust the maximum number of ARP attack detection logs for each log output. The logs that exceed the number limit will not be output and displayed.

An IRF member device can send a maximum of 128 ARP attack detection logs each time.

Examples

Enable ARP attack detection logging.

```
<Sysname> system-view
[Sysname] arp detection log enable
```

arp detection port-match-ignore

Use **arp detection port-match-ignore** to ignore ingress ports of ARP packets during user validity check.

Use **undo arp detection port-match-ignore** to remove the configuration.

Syntax

arp detection port-match-ignore

undo arp detection port-match-ignore

Default

Ingress ports of ARP packets are checked for user invalidity.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command configures ARP attack detection to ignore the ingress port information of ARP packets when the packets are compared with the entries used for user validity check.

Examples

Ignore ingress ports of ARP packets during user validity check.

```
<Sysname> system-view
[Sysname] arp detection port-match-ignore
```

Related commands

arp detection enable

arp detection rule

Use **arp detection rule** to configure a user validity check rule.

Use **undo arp detection rule** to delete a user validity check rule.

Syntax

arp detection rule *rule-id* { **deny** | **permit** } **ip** { *ip-address* [*mask*] | **any** } **mac** { *mac-address* [*mask*] | **any** } [**vlan** *vlan-id*]

undo arp detection rule [*rule-id*]

Default

No user validity check rule is configured.

Views

System view

Predefined user roles

network-admin

Parameters

rule-id: Assigns an ID to the user validity check rule. The ID value range is 0 to 511. A smaller value represents a higher priority.

deny: Denies matching ARP packets.

permit: Permits matching ARP packets.

ip { *ip-address* [*mask*] | **any** }: Specifies the sender IP address as the match criterion.

- *ip-address*: Specifies an IP address in dotted decimal notation.
- *mask*: Specifies the address mask in dotted decimal notation. If you do not specify the mask, the *ip-address* argument specifies a host IP address.
- **any**: Matches any IP address.

mac { *mac-address* [*mask*] | **any** }: Specifies the sender MAC address as the match criterion.

- *mac-address*: Specifies a MAC address in the H-H-H format.
- *mask*: Specifies the MAC address mask in the H-H-H format. If you do not specify the mask, the argument specifies the host MAC address.
- **any**: Matches any MAC address.

vlan *vlan-id*: Specifies the ID of a VLAN in the specified rule. The value range for the *vlan-id* argument is 1 to 4094. If you do not specify a VLAN, the packets' VLAN information is not checked.

Usage guidelines

A user validity check rule takes effect only when ARP attack detection is enabled.

If you do not specify a rule ID, the **undo arp detection rule** command deletes all user validity check rules.

Examples

Configure a user validity check rule and enable ARP detection for VLAN 2.

```
<Sysname> system-view
[Sysname] arp detection rule 0 permit ip 10.1.1.1 255.255.0.0 mac 0001-0203-0405
ffff-ffff-0000
[Sysname] vlan 2
[Sysname-vlan2] arp detection enable
```

Related commands

arp detection enable

arp detection trust

Use **arp detection trust** to configure an interface as an ARP trusted interface.

Use **undo arp detection trust** to restore the default.

Syntax

arp detection trust

undo arp detection trust

Default

An interface is an ARP untrusted interface.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Examples

Configure GigabitEthernet 1/0/1 as an ARP trusted interface.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp detection trust
```

arp detection validate

Use **arp detection validate** to enable ARP packet validity check.

Use **undo arp detection validate** to disable ARP packet validity check.

Syntax

arp detection validate { **dst-mac** | **ip** | **src-mac** } *

undo arp detection validate [**dst-mac** | **ip** | **src-mac**] *

Default

ARP packet validity check is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

dst-mac: Checks the target MAC address of ARP responses. If the target MAC address is all-zero, all-one, or inconsistent with the destination MAC address in the Ethernet header, the packet is considered invalid and discarded.

ip: Checks the sender and target IP addresses of ARP replies, and the sender IP address of ARP requests. All-one or multicast IP addresses are considered invalid and the corresponding packets are discarded.

src-mac: Checks whether the sender MAC address in the message body is identical to the source MAC address in the Ethernet header. If they are identical, the packet is forwarded. Otherwise, the packet is discarded.

Usage guidelines

You can specify more than one object to be checked in one command line.

If no keyword is specified, the **undo arp detection validate** command disables ARP packet validity check for all objects.

Examples

Enable ARP packet validity check by checking the MAC addresses and IP addresses of ARP packets.

```
<Sysname> system-view
[Sysname] arp detection validate dst-mac ip src-mac
```

arp restricted-forwarding enable

Use **arp restricted-forwarding enable** to enable ARP restricted forwarding.

Use **undo arp restricted-forwarding enable** to disable ARP restricted forwarding.

Syntax

arp restricted-forwarding enable

undo arp restricted-forwarding enable

Default

ARP restricted forwarding is disabled.

Views

VLAN view

Predefined user roles

network-admin

Examples

Enable ARP restricted forwarding in VLAN 2.

```
<Sysname> system-view
```

```
[Sysname] vlan 2
[Sysname-vlan2] arp restricted-forwarding enable
```

display arp detection

Use **display arp detection** to display the VLANs that are enabled with ARP attack detection.

Syntax

display arp detection

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the VLANs that are enabled with ARP attack detection.

```
<Sysname> display arp detection
ARP detection is enabled in the following VLANs:
1-2, 4-5
```

Table 3 Command output

Field	Description
ARP detection is enabled in the following VLANs:	VLANs enabled with ARP attack detection. If no VLANs are enabled with ARP attack detection, this field displays **ARP detection is not enabled in any VLANs.**.

Related commands

arp detection enable

display arp detection statistics attack-source

Use **display arp detection statistics attack-source** to display statistics for ARP attack sources.

Syntax

display arp detection statistics attack-source slot *slot-number*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its ID. If you do not specify a member device, this command displays ARP attack source statistics for the master device.

Examples

Display statistics for ARP attack sources on slot 1.

```
<Sysname> display arp detection statistics attack-source slot 1
Interface              VLAN  MAC address    IP address      Number     Time
GE1/0/1                1     0005-0001-0001 10.1.1.14       24         17:09:56
03-27-2017
```

Table 4 Command output

Field	Description
Interface	Receiving interface of ARP attack packets.
VLAN	VLAN to which ARP attack packets belong.
MAC address	Sender MAC address in ARP attack packets.
IP address	Sender IP address in ARP attack packets.
Number	Number of ARP attack packets dropped by ARP attack detection.
Time	The most recent time when ARP attack detection dropped an ARP attack packet.

Related commands

arp detection enable

display arp detection statistics packet-drop

Use **display arp detection statistics packet-drop** to display statistics for packets dropped by ARP attack detection.

Syntax

display arp detection statistics packet-drop [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays dropped packet statistics for all interfaces.

Usage guidelines

This command displays numbers of packets discarded by user validity check and ARP packet validity check on interfaces.

Examples

Display statistics for packets dropped by ARP attack detection.

```
<Sysname> display arp detection statistics packet-drop
State: U-Untrusted  T-Trusted
```

```
ARP packets dropped by ARP inspect checking:
Interface(State)            IP        Src-MAC   Dst-MAC   Inspect
GE1/0/1(U)                  40        0         0         78
GE1/0/2(U)                  0         0         0         0
GE1/0/3(T)                  0         0         0         0
GE1/0/4(U)                  0         0         30        0
```

Table 5 Command output

Field	Description
State	State of an interface: • **U**—ARP untrusted interface. • **T**—ARP trusted interface.
Interface(State)	Inbound interface of ARP packets. State specifies the port state, **trusted** or **untrusted**.
IP	Number of ARP packets discarded due to invalid sender and target IP addresses.
Src-MAC	Number of ARP packets discarded due to invalid source MAC address.
Dst-MAC	Number of ARP packets discarded due to invalid destination MAC address.
Inspect	Number of ARP packets that failed to pass user validity check.

Related commands

reset arp detection statistics packet-drop

reset arp detection statistics attack-source

Use **reset arp detection statistics attack-source** to clear statistics for ARP attack sources.

Syntax

reset arp detection statistics attack-source [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its ID. If you do not specify a member device, this command clears ARP attack source statistics for the master device.

Examples

Clear statistics for ARP attack sources.

```
<Sysname> reset arp detection statistics attack-source
```

Related commands

arp detection enable

display arp detection statistics attack-source

reset arp detection statistics packet-drop

Use **reset arp detection statistics packet-drop** to clear statistics for packets dropped by ARP attack detection.

Syntax

reset arp detection statistics packet-drop [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command clears dropped packet statistics for all interfaces.

Examples

Clear statistics for packets dropped by ARP attack detection.

```
<Sysname> reset arp detection statistics packet-drop
```

Related commands

display arp detection statistics packet-drop

ARP scanning and fixed ARP commands

arp fixup

Use **arp fixup** to convert existing dynamic ARP entries to static ARP entries.

Use **undo arp fixup** to convert valid static ARP entries to dynamic ARP entries and delete invalid static ARP entries.

Syntax

arp fixup

undo arp fixup

Views

System view

Predefined user roles

network-admin

Usage guidelines

The ARP conversion is a one-time operation. You can use this command again to convert the dynamic ARP entries learned later to static.

The static ARP entries converted from dynamic ARP entries have the same attributes as the manually configured static ARP entries. Due to the device's limit on the total number of static ARP entries, some dynamic ARP entries might fail the conversion.

The static ARP entries after conversion can include the following entries:

- Existing dynamic and static ARP entries before conversion.
- New dynamic ARP entries learned during the conversion.

Dynamic ARP entries that are aged out during the conversion are not converted to static ARP entries.

To delete a static ARP entry changed from a dynamic one, use the **undo arp** *ip-address* command. To delete all such static ARP entries, use the **reset arp all** or **reset arp static** command.

Examples

Convert existing dynamic ARP entries to static ARP entries.

```
<Sysname> system-view
[Sysname] arp fixup
```

arp scan

Use **arp scan** to trigger an ARP scanning in an address range.

Syntax

arp scan [*start-ip-address* **to** *end-ip-address*] [**send-rate** *pps*]

Views

VLAN interface view

Predefined user roles

network-admin

Parameters

start-ip-address: Specifies the start IP address of the scanning range.

end-ip-address: Specifies the end IP address of the scanning range. The end IP address must be higher than or equal to the start IP address.

send-rate *pps*: Specifies the rate at which the device sends ARP requests for ARP scanning, in pps. The value range for the *pps* argument is 10 to 1000, and the value must be a multiple of 10. If you do not set the rate, the device sends ARP requests to all IP addresses in the specified scanning range simultaneously.

Usage guidelines

CAUTION:

ARP scanning will take some time. To stop an ongoing scan, press **Ctrl** + **C**. Dynamic ARP entries are created based on ARP replies received before the scan is terminated.

ARP scanning automatically creates ARP entries for devices in the specified address range. IP addresses already in existing ARP entries are not scanned.

If the interface's primary and secondary IP addresses are in the address range, the sender IP address in the ARP request is the address on the smallest network segment.

If no address range is specified, the device learns ARP entries for devices on the subnet where the primary IP address of the interface resides. The sender IP address in the ARP requests is the primary IP address of the interface.

The start and end IP addresses must be on the same subnet as the primary IP address or secondary IP addresses of the interface.

You can set the ARP packet sending rate if the scanning range has a large number of IP addresses. This setting can avoid high CPU usage and heavy network load caused by a burst of ARP traffic.

When you set the sending rate to a large value, the device might use a rate lower than the specified rate to ensure the device performance.

Examples

Configure the device to scan the neighbors on the network where the primary IP address of VLAN-interface 2 resides.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] arp scan
```

Configure the device to scan neighbors in an address range.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] arp scan 1.1.1.1 to 1.1.1.20
```

Configure the device to scan neighbors in an address range on VLAN-interface 2 and set the ARP packet sending rate to 10 pps.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] arp scan 1.1.1.1 to 1.1.1.20 send-rate 10
```

ARP gateway protection commands

arp filter source

Use **arp filter source** to enable ARP gateway protection for a gateway.

Use **undo arp filter source** to disable ARP gateway protection for a gateway.

Syntax

arp filter source *ip-address*

undo arp filter source *ip-address*

Default

ARP gateway protection is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address of a protected gateway.

Usage guidelines

You can enable ARP gateway protection for a maximum of eight gateways on an interface.

You cannot configure both the **arp filter source** and **arp filter binding** commands on the same interface.

Examples

Enable ARP gateway protection for the gateway with IP address 1.1.1.1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp filter source 1.1.1.1
```

ARP filtering commands

arp filter binding

Use **arp filter binding** to enable ARP filtering and configure an ARP permitted entry.

Use **undo arp filter binding** to remove an ARP permitted entry.

Syntax

arp filter binding *ip-address mac-address*

undo arp filter binding *ip-address*

Default

ARP filtering is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

ip-address: Specifies a permitted sender IP address.

mac-address: Specifies a permitted sender MAC address.

Usage guidelines

If the sender IP and MAC addresses of an ARP packet match an ARP permitted entry, the ARP packet is permitted. If the sender IP and MAC addresses of an ARP packet do not match an ARP permitted entry, the ARP packet is discarded.

You can configure a maximum of eight ARP permitted entries on an interface.

You cannot configure both the **arp filter source** and **arp filter binding** commands on the same interface.

Examples

Enable ARP filtering and configure an ARP permitted entry.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp filter binding 1.1.1.1 0e10-0213-1023
```

Contents

ND attack defense commands

Source MAC consistency check commands

ipv6 nd check log enable

Use **ipv6 nd check log enable** to enable the ND logging feature.

Use **undo ipv6 nd check log enable** to restore the default.

Syntax

ipv6 nd check log enable

undo ipv6 nd check log enable

Default

The ND logging feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The ND logging feature logs source MAC inconsistency events, and sends the log messages to the information center. The information center can then output log messages from different source modules to different destinations. For more information about the information center, see *Network Management and Monitoring Configuration Guide*.

As a best practice, disable the ND logging feature to avoid excessive ND logs.

Examples

Enable the ND logging feature.

```
<Sysname> system-view
[Sysname] ipv6 nd check log enable
```

Related commands

ipv6 nd mac-check enable

ipv6 nd mac-check enable

Use **ipv6 nd mac-check enable** to enable source MAC consistency check for ND messages.

Use **undo ipv6 nd mac-check enable** to disable source MAC consistency check for ND messages.

Syntax

ipv6 nd mac-check enable

undo ipv6 nd mac-check enable

Default

Source MAC consistency check for ND messages is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Use this command to enable source MAC consistency check on a gateway. The gateway checks the source MAC address and the source link-layer address for consistency for each ND message. If an inconsistency is found, the gateway drops the ND message.

Examples

Enable source MAC consistency check for ND messages.

```
<Sysname> system-view
[Sysname] ipv6 nd mac-check enable
```

ND attack detection commands

display ipv6 nd detection statistics

Use **display ipv6 nd detection statistics** to display statistics for ND messages dropped by ND attack detection.

Syntax

display ipv6 nd detection statistics [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays statistics for ND messages dropped by ND attack detection on all interfaces.

Examples

Display statistics for all ND messages dropped by ND attack detection.

```
<Sysname> display ipv6 nd detection statistics
ND packets dropped by ND detection:
Interface/AC         Packets dropped
GE1/0/1              78
GE1/0/2              0
GE1/0/3              0
GE1/0/4              0
```

Table 1 Command output

Field	Description
Interface/AC	Input interface of the ND messages.
Packets dropped	Number of ND messages dropped by ND attack detection.

ipv6 nd detection enable

Use **ipv6 nd detection enable** to enable ND attack detection. This feature checks the ND message validity.

Use **undo ipv6 nd detection enable** to disable ND attack detection.

Syntax

ipv6 nd detection enable

undo ipv6 nd detection enable

Default

ND attack detection is disabled.

Views

VLAN view

Predefined user roles

network-admin

Examples

Enable ND attack detection for VLAN 10.

```
<Sysname> system-view
[Sysname] vlan 10
[Sysname-vlan10] ipv6 nd detection enable
```

ipv6 nd detection log enable

Use **ipv6 nd detection log enable** to enable ND attack detection logging.

Use **undo ipv6 nd detection log enable** to disable ND attack detection logging.

Syntax

ipv6 nd detection log enable

undo ipv6 nd detection log enable

Default

ND attack detection logging is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command allows a device to generate logs when it detects ND attacks. The log information helps administrators locate and solve problems. The ND attack detection logging feature sends the log message to the information center. The information center can then output log messages from different source modules to different destinations. For more information about information center, see *Network Management and Monitoring Configuration Guide*.

The device performance is degraded when the device outputs a large number of ND attack detection logs. You can disable ND attack detection logging to ensure the device performance.

Examples

Enable ND attack detection logging.

```
<Sysname> system-view
[Sysname] ipv6 nd detection log enable
```

ipv6 nd detection trust

Use **ipv6 nd detection trust** to configure an interface as an ND trusted interface.

Use **undo ipv6 nd detection trust** to restore the default.

Syntax

ipv6 nd detection trust

undo ipv6 nd detection trust

Default

All interfaces are ND untrusted interfaces.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Examples

Configure GigabitEthernet 1/0/1 as an ND trusted interface.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd detection trust
```

Configure Bridge-Aggregation 1 as an ND trusted interface.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] ipv6 nd detection trust
```

reset ipv6 nd detection statistics

Use **reset ipv6 nd detection statistics** to clear ND attack detection statistics.

Syntax

reset ipv6 nd detection statistics [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command clears ND attack detection statistics for all interfaces.

Examples

Clear all ND attack detection statistics.

```
<Sysname> reset ipv6 nd detection statistics
```

RA guard commands

display ipv6 nd raguard policy

Use **display ipv6 nd raguard policy** to display the RA guard policy configuration.

Syntax

display ipv6 nd raguard policy [*policy-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

policy-name: Specifies an RA guard policy by its name. The policy name is a case-sensitive string of 1 to 31 characters. If you do not specify a policy, this command displays the configuration of all RA guard policies.

Examples

Display the configuration of all RA guard policies.

```
<Sysname> display ipv6 nd raguard policy
Total number of policies: 2
RA Guard policy: policy1
  if-match ACL 2001
  if-match autoconfig managed-address-flag on
  if-match autoconfig other-flag off
  if-match hop-limit maximum 128
  if-match hop-limit minimum 100
  if-match prefix ACL name aa
  if-match router-preference medium
  applied to VLAN 1-3 7
RA Guard policy: policy2
  if-match ACL name zdd
```

```
if-match prefix ACL 2200
```

Table 2 Command output

Field	Description
RA Guard policy	Name of the RA guard policy.
if-match ACL	Number of the ACL in the ACL match criterion.
if-match ACL name	Name of the ACL in ACL match criterion.
if-match autoconfig managed-address-flag	Match criterion of the advertised M flag: • **on**—The value of the advertised M flag is 1. • **off**—The value of the advertised M flag is 0.
if-match autoconfig other-flag	Match criterion of the advertised O flag: • **on**—The value of the advertised O flag is 1. • **off**—The value of the advertised O flag is 0.
if-match hop-limit maximum	The maximum advertised hop limit match criterion.
if-match hop-limit minimum	The minimum advertised hop limit match criterion.
if-match prefix ACL	Number of the ACL used to identify the prefix match criterion.
if-match prefix ACL name	Name of the ACL used to identify the prefix match criterion.
applied to VLAN	ID of the VLAN to which the RA guard policy is applied.

Related commands

ipv6 nd raguard policy

display ipv6 nd raguard statistics

Use **display ipv6 nd raguard statistics** to display RA guard statistics.

Syntax

display ipv6 nd raguard statistics [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays RA guard statistics for all interfaces.

Examples

Display RA guard statistics.

```
<Sysname> display ipv6 nd raguard statistics
RA messages dropped by RA guard:
Interface    Dropped
GE1/0/1      78
```

```
GE1/0/2      0
GE1/0/3      32
GE1/0/4      0
```

Table 3 Command output

Field	Description
Interface	Interface that received the dropped RA messages.
Dropped	Number of RA messages dropped on the interface.

Related commands

ipv6 nd raguard log enable

reset ipv6 nd raguard statistics

if-match acl

Use **if-match acl** to specify an ACL match criterion.

Use **undo if-match acl** to delete the ACL match criterion.

Syntax

if-match acl { *ipv6-acl-number* | **name** *ipv6-acl-name* }

undo if-match acl

Default

No ACL match criterion exists.

Views

RA guard policy view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies an IPv6 basic ACL by its number in the range of 2000 to 2999.

name *ipv6-acl-name*: Specifies an IPv6 basic ACL by its name, a case-insensitive string of 1 to 63 characters. The name must start with an English letter. To avoid confusion, the name cannot be **all**.

Usage guidelines

RA guard uses the ACL match criterion to match the IP address of the RA message sender. If the sender IP address matches a permit rule, the message passes the check.

If the specified ACL does not exist or does not contain a rule, the ACL match criterion does not take effect.

Examples

Use IPv6 basic ACL 2001 as the ACL match criterion for RA guard policy **policy1**.

```
<Sysname> system-view
[Sysname] ipv6 nd raguard policy policy1
[Sysname-raguard-policy-policy1] if-match acl 2001
```

if-match autoconfig managed-address-flag

Use **if-match autoconfig managed-address-flag** to specify an M flag match criterion.

Use **undo if-match autoconfig managed-address-flag** to delete the M flag match criterion.

Syntax

if-match autoconfig managed-address-flag { **off** | **on** }

undo if-match autoconfig managed-address-flag

Default

No M flag match criterion exists.

Views

RA guard policy view

Predefined user roles

network-admin

Parameters

off: Specifies the advertised M flag as 0

on: Specifies the advertised M flag as 1.

Usage guidelines

The M flag in an RA message determines whether a receiving host uses stateful autoconfiguration to obtain an IPv6 address.

- If the M flag is set to 1, the host uses stateful autoconfiguration, for example, uses a DHCPv6 server.
- If the M flag is set to 0, the host uses stateless autoconfiguration. In stateless autoconfiguration, the host generates an IPv6 address according to its link-layer address and the prefix information in the RA message.

Examples

Specify **on** as the M flag match criterion for RA guard policy **policy1**.

```
<Sysname> system-view
[Sysname] ipv6 nd raguard policy policy1
[Sysname-raguard-policy-policy1] if-match autoconfig managed-address-flag on
```

if-match autoconfig other-flag

Use **if-match autoconfig other-flag** to specify an O flag match criterion.

Use **undo if-match autoconfig other-flag** to delete the O flag match criterion.

Syntax

if-match autoconfig other-flag { **off** | **on** }

undo if-match autoconfig other-flag

Default

No O flag match criterion exists.

Views

RA guard policy view

Predefined user roles

network-admin

Parameters

off: Specifies the advertised O flag as 0.

on: Specifies the advertised O flag as 1.

Usage guidelines

The O flag in an RA message determines whether a receiving host uses stateful autoconfiguration to obtain configuration information other than IPv6 address.

- If the O flag is set to 1, the host uses stateful autoconfiguration, for example, uses a DHCPv6 server.
- If the O flag is set to 0, the host uses stateless autoconfiguration.

Examples

Specify **on** as the M flag match criterion for RA guard policy **policy1**.

```
<Sysname> system-view
[Sysname] ipv6 nd raguard policy policy1
[Sysname-raguard-policy-policy1] if-match autoconfig other-flag on
```

if-match hop-limit

Use **if-match hop-limit** to specify a maximum or minimum hop limit match criterion.

Use **undo if-match hop-limit** to delete the maximum or minimum hop limit match criterion.

Syntax

if-match hop-limit { **maximum** | **minimum** } *limit*

undo if-match hop-limit { **maximum** | **minimum** }

Default

No maximum or minimum hop limit match criterion exists.

Views

RA guard policy view

Predefined user roles

network-admin

Parameters

maximum: Specifies the maximum advertised hop limit. An RA message passes the check if its current hop limit is not higher than the maximum advertised hop limit.

minimum: Specifies the minimum advertised hop limit. An RA message passes the check if its current hop limit is not less than the minimum advertised hop limit.

limit: Specifies the advertised hop limit in the range of 1 to 255.

Usage guidelines

If a hop limit match criterion is set, and the RA message's current hop limit is 0, the message will be dropped.

Examples

Set the maximum hop limit match criterion to 128 for RA guard policy **policy1**.

```
<Sysname> system-view
```

```
[Sysname] ipv6 nd raguard policy policy1
[Sysname-raguard-policy-policy1] if-match hop-limit maximum 128
```

if-match prefix

Use **if-match prefix** to specify a prefix match criterion.

Use **undo if-match prefix** to delete the prefix match criterion.

Syntax

if-match prefix acl { *ipv6-acl-number* | **name** *ipv6-acl-name* }

undo if-match prefix acl

Default

No prefix match criterion exists.

Views

RA guard policy view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies an IPv6 basic ACL by its number in the range of 2000 to 2999.

name *ipv6-acl-name*: Specifies an IPv6 basic ACL by its name, a case-insensitive string of 1 to 63 characters. The name must start with an English letter. To avoid confusion, the name cannot be **all**.

Usage guidelines

An RA message passes the check if the advertised prefixes in the message match the prefixes set by the ACL.

If the specified ACL does not exist or does not contain a rule, the prefix match criterion does not take effect.

Examples

Use IPv6 basic ACL 2000 as the prefix match criterion for RA guard policy **policy1**.

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2000
[Sysname-acl-ipv6-basic-2000] rule permit source 1001:: 64
[Sysname-acl-ipv6-basic-2000] rule permit source 3124:1123:: 64
[Sysname-acl-ipv6-basic-2000] rule deny source any
[Sysname-acl-ipv6-basic-2000] quit
[Sysname] ipv6 nd raguard policy policy1
[Sysname-raguard-policy-policy1] if-match prefix acl 2000
```

if-match router-preference

Use **if-match router-preference maximum** to specify a router preference match criterion.

Use **undo if-match router-preference maximum** to delete the router preference match criterion.

Syntax

if-match router-preference maximum { **high** | **low** | **medium** }

undo if-match router-preference maximum

Default

No router preference match criterion exists.

Views

RA guard policy view

Predefined user roles

network-admin

Parameters

high: Sets the maximum router preference to **high**. An RA message passes the check if its router preference is not higher than **high**.

low: Sets the maximum router preference to **low**. An RA message passes the check if its router preference is not higher than **low**.

medium: Sets the maximum router preference to **medium**. An RA message passes the check if its router preference is not higher than **medium**.

Usage guidelines

A host selects a router as the default gateway according to the router preference in received RA messages. If router preferences are the same, the host selects the default router from which the first RA message is received.

An RA message will not pass the router preference check if the message does not have a preference value. This RA message will be dropped.

Examples

Specify **medium** as the router preference match criterion for RA guard policy **policy1**.

```
<Sysname> system-view
[Sysname] ipv6 nd raguard policy policy1
[Sysname-raguard-policy-policy1] if-match router-preference maximum medium
```

ipv6 nd raguard apply policy

Use **ipv6 nd raguard apply policy** to apply an RA guard policy to a VLAN.

Use **undo ipv6 nd raguard apply policy** to remove the RA guard policy from a VLAN.

Syntax

ipv6 nd raguard apply policy [*policy-name*]

undo ipv6 nd raguard apply policy

Default

No RA guard policy is applied to a VLAN.

Views

VLAN view

Predefined user roles

network-admin

Parameters

policy-name: Specifies an RA guard policy by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a policy, RA guard blocks RA messages on all interfaces in the VLAN except interfaces that are defined to be connected to routers.

Usage guidelines

If an RA message has multiple VLAN tags, RA guard uses the outermost VLAN tag to select the applied RA guard policy.

If the specified RA guard policy does not exist, the command does not take effect.

Examples

Apply RA guard policy **policy1** to VLAN 100.

```
<Sysname> system-view
[Sysname] vlan 100
[Sysname-vlan100] ipv6 nd raguard apply policy policy1
```

Related commands

ipv6 nd raguard policy

ipv6 nd raguard log enable

Use **ipv6 nd raguard log enable** to enable the RA guard logging feature.

Use **undo ipv6 nd raguard log enable** to disable the RA guard logging feature.

Syntax

ipv6 nd raguard log enable

undo ipv6 nd raguard log enable

Default

The RA guard logging feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command allows a device to generate logs when it detects forged RA messages. The log information helps administrators locate and solve problems. Each log records the following information:

- Name of the interface that received the forged RA message.
- Source IP address of the forged RA message.
- Number of RA messages dropped on the interface.

The RA guard logging feature sends the log messages to the information center. The information center can then output log messages from different source modules to different destinations. For more information about the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Enable the RA guard logging feature.

```
<Sysname> system-view
```

```
[Sysname] ipv6 nd raguard log enable
```

Related commands

display ipv6 nd raguard statistics

reset ipv6 nd raguard statistics

ipv6 nd raguard policy

Use **ipv6 nd raguard policy** to create an RA guard policy and enter its view, or enter the view of an existing RA guard policy.

Use **undo ipv6 nd raguard policy** to delete an RA guard policy.

Syntax

ipv6 nd raguard policy *policy-name*

undo ipv6 nd raguard policy *policy-name*

Default

No RA guard policies exist.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Assigns a name to the RA guard policy. The name is a case-sensitive string of 1 to 31 characters.

Examples

Create RA guard policy **policy1** and enter its view.

```
<Sysname> system-view
[Sysname] ipv6 nd raguard policy policy1
[Sysname-raguard-policy-policy1]
```

Related commands

display ipv6 nd raguard policy

ipv6 nd raguard apply policy

ipv6 nd raguard role

Use **ipv6 nd raguard role** to specify the role of the device attached to the interface.

Use **undo ipv6 nd raguard role** to remove the role of the device attached to the interface.

Syntax

ipv6 nd raguard role { **host** | **router** }

undo ipv6 nd raguard role

Default

No role is specified for the device attached to the interface.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

host: Specifies the host role. The interface attached to a host drops all received RA messages.

router: Specifies the router role. The interface attached to a router forwards all received RA messages.

Usage guidelines

Make sure your setting is consistent with the device type. If you are not aware of the attached device type, do not specify a role for the device.

Examples

Specify **host** as the role for the device attached to GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd raguard role host
```

reset ipv6 nd raguard statistics

Use **reset ipv6 nd raguard statistics** to clear RA guard statistics.

Syntax

reset ipv6 nd raguard statistics [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command clears RA guard statistics for all interfaces.

Examples

Clear RA guard statistics.

```
<Sysname> reset ipv6 nd raguard statistics
```

Related commands

display ipv6 nd raguard statistics

Contents

SAVI commands

ipv6 savi down-delay

Use **ipv6 savi down-delay** to set the entry deletion delay.

Use **undo ipv6 savi down-delay** to restore the default.

Syntax

ipv6 savi down-delay *delay-time*

undo ipv6 savi down-delay

Default

The entry deletion delay is 30 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

delay-time: Specifies the entry deletion delay in the range of 0 to 21474836 seconds.

Usage guidelines

The entry deletion delay is the period of time that the device waits before deleting the DHCPv6 snooping entries and ND snooping entries for a down port.

Examples

Set the entry deletion delay to 100 seconds.

```
<Sysname> system-view
[Sysname] ipv6 savi down-delay 100
```

ipv6 savi log enable

Use **ipv6 savi log enable** to enable packet spoofing logging or filtering entry logging.

undo ipv6 savi log enable to disable packet spoofing logging or filtering entry logging.

NOTE:

This command is supported only in Release 6328 and later.

Syntax

ipv6 savi log enable { **spoofing-packet** [**interval** *interval* | **total-number** *number*] * | **filter-entry** }

undo ipv6 savi log enable { **spoofing-packet** | **filter-entry** }

Default

Packet spoofing logging and filtering entry logging are disabled.

Views

System view

Predefined user roles

network-admin

network-operator

Parameters

spoofing-packet [**interval** *interval* | **total-number** *number*]: Enables packet spoofing logging.

- **interval** *interval*: Sets the log output interval in seconds. The value of the *interval* argument can be 0 or in the range of 5 to 3600. The default value is 60 seconds. If you set this parameter to 0, the device outputs a log message immediately after it is generated.
- **total-number** *number*: Sets the maximum number of log messages that can be output per interval. The value range for the *number* argument is 1 to 128, and the default value is 128.

filter-entry: Enables filtering entry logging.

Usage guidelines

Packet spoofing logging enables the device to generate log messages for the spoofed packets detected by SAVI.

Filtering entries are effective bindings used for filtering IPv6 packets by the source IPv6 address. Filtering entry logging enables the device to generate log messages for filtering entries. A log message contains the IPv6 address, MAC address, VLAN, and interface of a filtering entry.

The device sends packet spoofing and filtering entry log messages to the information center. With the information center, you can set log message filtering and output rules, including output destinations. For more information about using the information center, see *Network Management and Monitoring Configuration Guide*.

The device can output a maximum of 128 packet spoofing log messages. If this limit is crossed, the device drops excess log messages. To ensure device performance, set the log output interval and maximum number of log messages output per interval appropriately.

Examples

Enable packet spoofing logging.

```
<Sysname> system-view
[Sysname] ipv6 savi log enable spoofing-packet
```

ipv6 savi strict

Use **ipv6 savi strict** to enable Source Address Validation Improvement (SAVI).

Use **undo ipv6 savi strict** to disable SAVI.

Syntax

ipv6 savi strict

undo ipv6 savi strict

Default

SAVI is disabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable SAVI.

```
<Sysname> system-view
[Sysname] ipv6 savi strict
```

Related commands

ipv6 verify source

Contents

MFF commands

display mac-forced-forwarding interface

Use **display mac-forced-forwarding interface** to display MFF port configuration.

Syntax

display mac-forced-forwarding interface

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display MFF port configuration.

```
<Sysname> display mac-forced-forwarding interface
Network Port:
GE1/0/1                 GE1/0/2
User Port:
GE1/0/3                 GE1/0/4                 GE1/0/5
...
```

Table 1 Command output

Field	Description
Network Port	List of network ports.
User Port	List of user ports.

Related commands

mac-forced-forwarding network-port

display mac-forced-forwarding vlan

Use **display mac-forced-forwarding vlan** to display the MFF configuration for a VLAN.

Syntax

display mac-forced-forwarding vlan *vlan-id*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan-id: Specifies a VLAN by its ID.

Examples

Display the MFF configuration for VLAN 2.

```
<Sysname> display mac-forced-forwarding vlan 2
VLAN 2
Gateway:
------------------------------------------------------------------------
192.168.1.42         000f-e200-8046
Server:
------------------------------------------------------------------------
192.168.1.48         192.168.1.49
```

Table 2 Command output

Field	Description
VLAN 2	ID of the VLAN to which the gateways belong.
Gateway	IP and MAC addresses of gateways. If no address is learned, this field displays **N/A**.
Server	Server IP addresses.

Related commands

mac-forced-forwarding

mac-forced-forwarding server

mac-forced-forwarding

Use **mac-forced-forwarding** to enable MFF and specify the default gateway.

Use **undo mac-forced-forwarding** to disable MFF.

Syntax

mac-forced-forwarding default-gateway *gateway-ip*

undo mac-forced-forwarding

Default

MFF is disabled.

Views

VLAN view

Predefined user roles

network-admin

Parameters

default-gateway *gateway-ip*: Specifies the IP address of the default gateway.

Usage guidelines

For MFF to take effect, make sure ARP snooping is enabled on the VLAN where MFF is enabled.

For a network (or VLAN) with IP addresses manually configured, the gateway IP address must be manually configured. MFF checks for and denies only all-zero and all-one gateway IP addresses.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Enable MFF for VLAN 2 and specify the IP address of the default gateway.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] mac-forced-forwarding default-gateway 1.1.1.1
```

Related commands

mac-forced-forwarding server

mac-forced-forwarding gateway probe

Use **mac-forced-forwarding gateway probe** to enable periodic gateway probe.

Use **undo mac-forced-forwarding gateway probe** to disable periodic gateway probe.

Syntax

mac-forced-forwarding gateway probe

undo mac-forced-forwarding gateway probe

Default

Periodic gateway probe is disabled.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

Make sure you have enabled MFF before enabling periodic gateway probe. The probe interval is 30 seconds.

Examples

Enable periodic gateway probe.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] mac-forced-forwarding gateway probe
```

Related commands

mac-forced-forwarding

mac-forced-forwarding network-port

Use **mac-forced-forwarding network-port** to configure the Ethernet port as a network port.

Use **undo mac-forced-forwarding network-port** to restore the default.

Syntax

mac-forced-forwarding network-port

undo mac-forced-forwarding network-port

Default

The Ethernet port is a user port.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

You should configure the following ports as network ports:

- Upstream ports connected to a gateway.
- Ports connected to the MFF devices in a cascaded network (a network with multiple MFF devices connected to one another).
- Ports between devices in a ring network.

You can configure multiple ports as network ports.

You can configure a port as a network port regardless of whether MFF is enabled for the VLAN of the port. However, the configuration takes effect only after MFF is enabled.

Link aggregation is supported by network ports in an MFF-enabled VLAN, but is not supported by user ports in the VLAN. To cancel the network port configuration of a link aggregation member port in a MFF-enabled VLAN, remove the network port from the link aggregation group first. For more information about link aggregation, see *Layer 2—LAN Switching Configuration Guide*.

Examples

Configure GigabitEthernet 1/0/1 as a network port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-forced-forwarding network-port
```

Related commands

mac-forced-forwarding

mac-forced-forwarding server

Use **mac-forced-forwarding server** to specify the IP addresses of servers.

Use **undo mac-forced-forwarding server** to remove server IP addresses.

Syntax

mac-forced-forwarding server *server-ip*&<1-10>

undo mac-forced-forwarding server *server-ip*&<1-10>

Default

No server IP address is specified.

Views

VLAN view

Predefined user roles

network-admin

Parameters

server-ip&<1-10>: Specifies a space-separated list of up to 10 server IP addresses.

Usage guidelines

You need to maintain a server list on the MFF device to ensure communication between the servers and clients.

Server IP addresses can be those of the servers collaborating with MFF, such as a RADIUS server.

When the MFF device receives an ARP request from a server, it searches the IP-to-MAC address entries it has stored. Then the device replies with the requested MAC address to the server.

In this way, packets from the server to a host are not forwarded by the gateway. However, packets from a host to the server are forwarded by the gateway.

MFF does not check whether the IP address of a server is on the same network segment as that of a gateway. Instead, it checks whether the IP address of a server is all-zero or all-one. An all-zero or all-one server IP address is invalid.

Make sure MFF is enabled before you execute the **mac-forced-forwarding server** command.

Examples

Specify the server at 192.168.1.100.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] mac-forced-forwarding server 192.168.1.100
```

Related commands

mac-forced-forwarding

Contents

Crypto engine commands

display crypto-engine

Use **display crypto-engine** to display crypto engine information.

Syntax

display crypto-engine

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display crypto engine information.

```
<Sysname> display crypto-engine
  Crypto engine name: Software crypto engine
  Crypto engine state: Enabled
  Crypto engine type: Software
  Slot ID: 1
  CPU ID:0
  Crypto engine ID: 0
  Symmetric algorithms:  des-cbc des-ecb 3des-cbc aes-cbc aes-ecb aes-ctr camellia_cbc
md5 sha1 sha2-256 sha2-384 sha2-512 md5-hmac sha1-hmac sha2-256-hmac sha2-384-hmac
sha2-512-hmac aes-xcbc aes-xcbc-hmac
  Asymmetric algorithms:
  Random number generation function: Supported
```

Table 1 Command output

Field	Description
Crypto engine state	This field always displays **Enabled** for software crypto engines.
Crypto engine type	The value is **Software** for this field.
CPU ID	ID of the CPU on the device.
Symmetric algorithms	Supported symmetric algorithms.
Asymmetric algorithms	Supported asymmetric algorithms.
Random number generation function	Whether random number generation function is supported: • Supported. • Not supported.

display crypto-engine statistics

Use **display crypto-engine statistics** to display crypto engine statistics.

Syntax

display crypto-engine statistics [**engine-id** *engine-id* **slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

engine-id *engine-id*: Specifies a crypto engine by its ID. The switch supports only one software crypto engine, and the engine ID can only be 0.

slot *slot-number*: Specifies an IRF member device by its member ID.

Usage guidelines

If you do not specify any parameters, this command displays crypto engine statistics for all member devices.

Examples

Display all crypto engine statistics.

```
<Sysname> display crypto-engine statistics
  Slot ID: 1
  CPU ID: 0
  Crypto engine ID: 0
  Submitted sessions: 0
  Failed sessions: 0
  Symmetric operations: 0
  Symmetric errors: 0
  Asymmetric operations: 0
  Asymmetric errors: 0
  Get-random operations: 0
  Get-random errors: 0
```

Table 2 Command output

Field	Description
Submitted sessions	Number of established sessions.
Failed sessions	Number of failed sessions.
Symmetric operations	Number of operations using symmetric algorithms.
Symmetric errors	Number of failed operations using symmetric algorithms.
Asymmetric operations	Number of operations using asymmetric algorithms.
Asymmetric errors	Number of failed operations using asymmetric algorithms.
Get-random operations	Number of operations for obtaining random numbers.
Get-random errors	Number of failed operations for obtaining random numbers.

Related commands

reset crypto-engine statistics

reset crypto-engine statistics

Use **reset crypto-engine statistics** to clear crypto engine statistics.

Syntax

reset crypto-engine statistics [**engine-id** *engine-id* **slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

Parameters

engine-id *engine-id*: Specifies a crypto engine by its ID. The switch supports only one software crypto engine, and the engine ID can only be 0.

slot *slot-number*: Specifies an IRF member device by its member ID.

Usage guidelines

If you do not specify any parameters, this command clears crypto engine statistics for all member devices.

Examples

Clear statistics for all crypto engines.

```
<Sysname> reset crypto-engine statistics
```

Related commands

display crypto-engine statistics

Contents

FIPS commands

display crypto version

Use **display crypto version** to display the version number of the device algorithm base.

Syntax

display crypto version

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

Each algorithm base version number represents a set of cryptographic algorithms.

Examples

Display the version number of the current device algorithm base.

```
<Sysname> display crypto version
7.1.1.1.1.72
```

Table 1 Command output

Field	Description
7.1.1.1.1.72	Version number in the **7.1.***X* format. • **7.1**—Comware V700R001. • **X**—Version number of the device algorithm base.

display fips status

Use **display fips status** to display the FIPS mode state.

Syntax

display fips status

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the FIPS mode state.

```
<Sysname> display fips status
FIPS mode is enabled.
```

Related commands

fips mode enable

fips mode enable

Use **fips mode enable** to enable FIPS mode.

Use **undo fips mode enable** to disable FIPS mode.

Syntax

fips mode enable

undo fips mode enable

Default

FIPS mode is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

CAUTION:

- When you enable or disable FIPS mode, the system prompts you to select the reboot method before it reboots. System reboot might interrupt ongoing services. Perform this operation with caution.
- If you select the manual reboot method to enable FIPS mode, you must manually complete the configurations for entering FIPS mode. If you fail to do so, the system enters FIPS mode after reboot but you cannot log in to the system correctly.

After you enable FIPS mode and reboot the device, the device operates in FIPS mode. The FIPS device has strict security requirements, and performs self-tests on cryptography modules to verify that they are operating correctly.

After you execute the **fips mode enable** command, the system provides the following methods to enter FIPS mode:

- Automatic reboot

  Select the automatic reboot method. The system automatically performs the following operations:

  a. Create a default FIPS configuration file named **fips-startup.cfg**.

  b. Specify the default file as the startup configuration file.

  c. Require you to configure the username and password for next login.

  After you configure the username and password at prompt, the system automatically uses the specified startup configuration file to reboot the device.

  During the interactive configuration process, you can press **Ctrl+C** to abort the configuration process and the **fips mode enable** command.

- Manual reboot

  This method requires that you manually complete the configurations for entering FIPS mode, and then reboot the device.

  To use manual reboot to enter FIPS mode:

  a. Enable the password control feature globally.

b. Set the number of character types a password must contain to 4, and set the minimum number of characters for each type to one character.

c. Set the minimum length of user passwords to 15 characters.

d. Add a local user account for device management, including the following items:

- A username.
- A password that must comply with the password control policies.
- A user role of **network-admin**.
- A service type of **terminal**.

e. Delete the FIPS-incompliant local user service types Telnet, HTTP, and FTP.

f. Save the configuration file and specify it as the startup configuration file.

g. Delete the original startup configuration file in binary format.

h. Reboot the device.

After executing the **`fips mode enable`** command, the system prompts you to choose a reboot method. If you do not make a choice within 30 seconds, the system uses the manual reboot method by default.

After executing the **`undo fips mode enable`** command, the system provides the following methods to exit FIPS mode:

- Automatic reboot

  Select the automatic reboot method. The system automatically creates a default non-FIPS configuration file named **non-fips-startup.cfg**, and specifies the file as the startup configuration file. The system reboots the device by using the default non-FIPS configuration file. After the reboot, you are directly logged into the device.

- Manual reboot

  This method requires that you manually complete the configurations for entering non-FIPS mode, and then reboot the device. After the device reboots, you must enter user information according to the authentication mode to log in to the device.

Examples

Enable FIPS mode, and choose the automatic reboot method to enter FIPS mode.

```
<Sysname> system-view
[Sysname] fips mode enable
FIPS mode change requires a device reboot. Continue? [Y/N]:y
Reboot the device automatically? [Y/N]:y
The system will create a new startup configuration file for FIPS mode. After you set the login username and password for FIPS mode, the device will reboot automatically.
Enter username(1-55 characters): root
Enter password(15-63 characters):
Confirm password:
Waiting for reboot... After reboot, the device will enter FIPS mode.
```

Enable FIPS mode, and choose the manual reboot method to enter FIPS mode.

```
<Sysname> system-view
[Sysname] fips mode enable
FIPS mode change requires a device reboot. Continue? [Y/N]:y
Reboot the device automatically? [Y/N]:n
Change the configuration to meet FIPS mode requirements, save the configuration to the next-startup configuration file, and then reboot to enter FIPS mode.
```

Disable FIPS mode, and choose the automatic reboot method to enter non-FIPS mode.

```
[Sysname] undo fips mode enable
```

```
FIPS mode change requires a device reboot. Continue? [Y/N]:y
The system will create a new startup configuration file for non-FIPS mode and then reboot automatically. Continue? [Y/N]:y
Waiting for reboot... After reboot, the device will enter non-FIPS mode.
```

Disable FIPS mode, and choose the manual reboot method to enter non-FIPS mode.

```
[Sysname] undo fips mode enable
FIPS mode change requires a device reboot. Continue? [Y/N]:y
The system will create a new startup configuration file for non-FIPS mode, and then reboot automatically. Continue? [Y/N]:n
Change the configuration to meet non-FIPS mode requirements, save the configuration to the next-startup configuration file, and then reboot to enter non-FIPS mode.
```

Related commands

`display fips status`

fips self-test

Use **`fips self-test`** to trigger a self-test on the cryptographic algorithms.

Syntax

`fips self-test`

Views

System view

Predefined user roles

network-admin

Usage guidelines

CAUTION:

A successful self-test requires that all cryptographic algorithms pass the self-test. If the self-test fails, the device where the self-test process exists reboots.

This command is supported only in FIPS mode. To examine whether the cryptography modules operate correctly, you can use this command to trigger a self-test on the cryptographic algorithms. The triggered self-test is the same as the power-up self-test.

Examples

Trigger a self-test on the cryptographic algorithms.

```
<Sysname> system-view
[Sysname] fips self-test
Cryptographic Algorithms Known-Answer Tests are running ...
Slot 1:
Starting Known-Answer tests in the user space.
Known-answer test for 3DES passed.
Known-answer test for SHA1 passed.
Known-answer test for SHA224 passed.
Known-answer test for SHA256 passed.
Known-answer test for SHA384 passed.
Known-answer test for SHA512 passed.
Known-answer test for HMAC-SHA1 passed.
Known-answer test for HMAC-SHA224 passed.
```

```
Known-answer test for HMAC-SHA256 passed.
Known-answer test for HMAC-SHA384 passed.
Known-answer test for HMAC-SHA512 passed.
Known-answer test for AES passed.
Known-answer test for RSA(signature/verification) passed.
Pairwise conditional test for RSA(signature/verification) passed.
Pairwise conditional test for RSA(encrypt/decrypt) passed.
Pairwise conditional test for DSA(signature/verification) passed.
Pairwise conditional test for ECDSA(signature/verification) passed.
Known-answer test for ECDH passed.
Known-answer test for random number generator(x931) passed.
Known-answer test for DRBG passed.
Known-Answer tests in the user space passed.
Starting Known-Answer tests in the kernel.
Known-answer test for 3DES passed.
Known-answer test for AES passed.
Known-answer test for HMAC-SHA1 passed.
Known-answer test for HMAC-SHA256 passed.
Known-answer test for HMAC-SHA384 passed.
Known-answer test for HMAC-SHA512 passed.
Known-answer test for SHA1 passed.
Known-answer test for SHA256 passed.
Known-answer test for SHA384 passed.
Known-answer test for SHA512 passed.
Known-answer test for GCM passed.
Known-answer test for GMAC passed.
Known-Answer tests in the kernel passed.
Cryptographic Algorithms Known-Answer Tests passed.
```

Contents

802.1X client commands

display dot1x supplicant

Use **display dot1x supplicant** to display 802.1X authentication information about 802.1X clients.

Syntax

display dot1x supplicant [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays 802.1X authentication information about 802.1X clients on all interfaces.

Examples

Display 802.1X authentication information about 802.1X clients on GigabitEthernet 1/0/1.

```
<Sysname> display dot1x supplicant interface gigabitethernet 1/0/1
GigabitEthernet1/0/1
  Username             : aaa
  EAP method           : PEAP-MSCHAPv2
  Dot1x supplicant     : Enabled
  Anonymous identifier : bbb
  SSL client policy    : policy_1
  FSM state            : Init
  EAPOL-Start packets  : 0
```

Table 1 Command output

Field	Description
Username	802.1X client username.
EAP method	802.1X client EAP authentication method: • MD5. • PEAP-GTC. • PEAP-MSCHAPv2. • TTLS-GTC. • TTLS-MSCHAPv2.
Dot1x supplicant	Status of the 802.1X client feature: • Enabled. • Disabled.
Anonymous identifier	802.1X client anonymous identifier.

Field	Description
SSL client policy	SSL client policy used by the 802.1X client feature.
FSM state	802.1X client authentication state: • **Init**—The authentication process starts. • **Connecting**—The 802.1X client is connecting to the authenticator. • **Authenticating**—The 802.1X client is being authenticated. • **Authenticated**—The 802.1X client has been authenticated. • **Held**—The 802.1X client is waiting for authentication.
EAPOL-Start packets	Number of sent EAPOL-Start packets.

dot1x supplicant anonymous identify

Use **dot1x supplicant anonymous identify** to configure an 802.1X client anonymous identifier.

Use **undo dot1x supplicant anonymous identify** to restore the default.

Syntax

dot1x supplicant anonymous identify *identifier*

undo dot1x supplicant anonymous identify

Default

No 802.1X client anonymous identifier exists.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

identifier: Specifies an 802.1X client anonymous identifier, a case-sensitive string of 1 to 253 characters.

Usage guidelines

At the first authentication phase, packets sent to the authenticator are not encrypted. The use of an 802.1X client anonymous identifier prevents the 802.1X client username from being disclosed at the first phase. The 802.1X client-enabled device sends the anonymous identifier to the authenticator instead of the 802.1X client username. The 802.1X client username will be sent to the authenticator in encrypted packets at the second phase.

If no 802.1X client anonymous identifier is configured, the device sends the 802.1X client username in the first phase.

The configured 802.1X client anonymous identifier takes effect only if one of the following EAP authentication methods is used:

- PEAP-MSCHAPv2.
- PEAP-GTC.
- TTLS-MSCHAPv2.
- TTLS-GTC.

If the MD5-Challenge EAP authentication is used, the configured 802.1X client anonymous identifier does not take effect. The device uses the 802.1X client username at the first authentication phase.

Do not configure the 802.1X client anonymous identifier if the vendor-specific authentication server cannot identify anonymous identifiers.

Examples

Configure the 802.1X client anonymous identifier as **bbb** on a port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x supplicant anonymous identify bbb
```

Related commands

display dot1x supplicant

dot1x supplicant enable

dot1x supplicant username

dot1x supplicant eap-method

Use **dot1x supplicant eap-method** to specify an 802.1X client EAP authentication method.

Use **undo dot1x supplicant eap-method** to restore the default.

Syntax

dot1x supplicant eap-method { **md5** | **peap-gtc** | **peap-mschapv2** | **ttls-gtc** | **ttls-mschapv2** }

undo dot1x supplicant eap-method

Default

The MD5-Challenge authentication is used as the 802.1X client EAP authentication method.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

md5: Specifies the MD5-challenge EAP authentication method.

peap-gtc: Specifies the PEAP-GTC EAP authentication method.

peap-mschapv2: Specifies the PEAP-MSCHAPv2 EAP authentication method

ttls-gtc: Specifies the TTLS-GTC EAP authentication method.

ttls-mschapv2: Specifies the TTLS-MSCHAPv2 EAP authentication method.

Usage guidelines

Make sure the specified 802.1X client EAP authentication method is supported by the authentication server.

Examples

Specify PEAP-GTC as the 802.1X client EAP authentication method on a port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] dot1x supplicant eap-method peap-gtc
```

Related commands

display dot1x supplicant

dot1x supplicant enable

dot1x supplicant enable

Use **dot1x supplicant enable** to enable the 802.1X client feature.

Use **undo dot1x supplicant enable** to disable the 802.1X client feature.

Syntax

dot1x supplicant enable

undo dot1x supplicant enable

Default

The 802.1X client feature is disabled.

Views

Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

Make sure you have configured 802.1X authentication on the authenticator before you use this command.

Examples

Enable the 802.1X client feature on a port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x supplicant enable
```

Related commands

display dot1x supplicant

dot1x supplicant mac-address

Use **dot1x supplicant mac-address** to configure an 802.1X client MAC address on an interface.

Use **undo dot1x supplicant mac-address** to restore the default.

Syntax

dot1x supplicant mac-address *mac-address*

undo dot1x supplicant mac-address

Default

The 802.1X client on an Ethernet interface uses the interface's MAC address for 802.1X authentication. If the interface's MAC address is unavailable, the 802.1X client uses the device's MAC address for 802.1X authentication.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

mac-address: Specifies a MAC address in the format of H-H-H, excluding multicast, all-zero, and all-F MAC addresses. When entering a MAC address, you can omit the leading zeros in each H section. For example, enter f-e2-1 for 000f-00e2-0001.

Usage guidelines

If multiple Ethernet interfaces on the device act as 802.1X clients, configure a unique MAC address for each interface to ensure that they can pass 802.1X authentication.

You can use either of the following methods to configure a unique MAC address for each 802.1X client-enabled interface:

- Execute the **mac-address** command in Ethernet interface view.
- Execute the **dot1x supplicant mac-address** command.

Examples

Configure the 802.1X client MAC address as 0001-0001-0001 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x supplicant mac-address 1-1-1
```

dot1x supplicant password

Use **dot1x supplicant password** to set an 802.1X client password.

Use **undo dot1x supplicant password** to restore the default.

Syntax

dot1x supplicant password { **cipher** | **simple** } *string*

undo dot1x supplicant password

Default

No 802.1X client password exists.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 127 characters. Its encrypted form is a case-sensitive string of 1 to 201 characters.

Examples

Set the 802.1X client password to **123456** in plaintext form on a port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x supplicant password simple 123456
```

Related commands

display dot1x supplicant

dot1x supplicant enable

dot1x supplicant ssl-client-policy

Use **dot1x supplicant ssl-client-policy** to specify an SSL client policy for an 802.1X client-enabled device.

Use **undo dot1x supplicant ssl-client-policy** to restore the default.

Syntax

dot1x supplicant ssl-client-policy *policy-name*

undo dot1x supplicant ssl-client-policy *policy-name*

Default

An 802.1X client-enabled device uses the default SSL client policy.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

policy-name: Specifies an SSL client policy by its name, a case-insensitive string of 1 to 31 characters. Make sure the specified SSL client policy already exists.

Usage guidelines

If the PEAP-MSCHAPv2, PEAP-GTC, TTLS-MSCHAPv2, or TTLS-GTC authentication is used, the 802.1X authentication process is as follows:

- **The first phase**—The device acts as an SSL client to negotiate with the SSL server.

  The SSL client uses the SSL parameters specified in the specified SSL client policy to establish a connection to the SSL server for negotiation. The SSL parameters include a PKI domain, supported cipher suites, and the SSL version. For information about SSL client policies, see *Security Configuration Guide*.
- **The second phase**—The device uses the negotiated result to encrypt and transmit the interchanged authentication packets.

If the MD5-Challenge authentication is used, the device does not use an SSL client policy during the authentication process.

Examples

Specify SSL client policy **policy_1** to be used by an 802.1X client-enabled device on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x supplicant ssl-client-policy policy_1
```

Related commands

display dot1x supplicant

dot1x supplicant enable

ssl client-policy

dot1x supplicant transmit-mode

Use **dot1x supplicant transmit-mode** to specify a mode used by 802.1X authentication for sending EAP-Response and EAPOL-Logoff packets.

Use undo dot1x supplicant transmit-mode to restore the default.

Syntax

dot1x supplicant transmit-mode { **multicast** | **unicast** }

undo dot1x supplicant transmit-mode

Default

802.1X authentication uses unicast mode to send EAP-Response and EAPOL-Logoff packets.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

multicast: Specifies multicast mode for sending EAP-Response and EAPOL-Logoff packets, of which the destination addresses are multicast MAC address 01-80-C2-00-00-03.

unicast: Specifies unicast mode for sending EAP-Response and EAPOL-Logoff packets.

Usage guidelines

When the device acts as an 802.1X client, use the multicast mode to avoid 802.1X authentication failures if the NAS device does not support receiving unicast EAP-Response or EAPOL-Logoff packets.

Examples

Configure 802.1X authentication to use multicast mode for sending EAP-Response and EAPOL-Logoff packets on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x supplicant transmit-mode multicast
```

dot1x supplicant username

Use **dot1x supplicant username** to configure an 802.1X client username.

Use **undo dot1x supplicant username** to restore the default.

Syntax

dot1x supplicant username *username*

undo dot1x supplicant username

Default

No 802.1X client username exists.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

username: Specifies the 802.1X client username, a case-sensitive string of 1 to 253 characters.

Usage guidelines

802.1X client usernames can include domain names. The supported domain name delimiters include the at sign (@), backslash (\), dot (.), and forward slash (/). Usernames that include domain names can use the format of *username*@*domain-name*, *domain-name**username*, *username*.*domain-name*, or *username*/*domain-name*.

If you want to use backslash (\) as the domain name delimiter, you must enter the escape character (\) along with the backslash (\) sign.

If a username string includes multiple configured delimiters, the device takes the rightmost delimiter in the username string as the domain name delimiter. For more information about the domain name delimiters, see the **dot1x domain-delimiter** command.

Examples

Configure the 802.1X client username as **aaa** on a port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x supplicant username aaa
```

Related commands

display dot1x supplicant

dot1x domain-delimiter

dot1x supplicant enable

High Availability Command Reference

This command reference is applicable to the following switches and software versions:

H3C S5120V2-LI switch series (Release 6308P01 and later)
H3C S3100V3-SI switch series (Release 6309P01 and later)
H3C S5110V2 switch series (Release 6310 and later)
H3C S5110V2-SI switch series (Release 6310 and later)
H3C S5000V3-EI switch series (Release 6310 and later)
H3C S5000V5-EI switch series (Release 6319P01 and later)
H3C S5000E-X switch series (Release 6310 and later)
H3C S5130S-LI switch series (Release 6310 and later)
H3C MS4320V2 switch series (Release 6308P01 and later)
H3C MS4320 switch series (Release 6308P01 and later)
H3C MS4300V2 switch series (Release 6308P01 and later)
H3C MS4200 switch series (Release 6310 and later)
H3C WS5810-WiNet switch series (Release 6308P01 and later)
H3C WS5820-WiNet switch series (Release 6308P01 and later)
H3C WAS6000 switch series (Release 6308P01 and later)
H3C S5000X-EI switch series (Release 6329 and later)
H3C MS4320V3 switch series (Release 6329 and later)
H3C S5120V3-SI switch series (Release 6329 and later)
H3C S5120V3-LI switch series (Release 6329 and later)

New H3C Technologies Co., Ltd.
http://www.h3c.com

Software version: Release 63xx
Document version: 6W105-20230524

Preface

This command reference describes fault detection and fast failover configuration commands. With these commands, you can detect and diagnose your network, and rapidly recover your network when failures occur.

This preface includes the following topics about the documentation:

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** >

Convention	Description
	Folder.

Symbols

Convention	Description
⚠ **WARNING!**	An alert that calls attention to important information that if not understood or followed can result in personal injury.
△ **CAUTION:**	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
ⓘ **IMPORTANT:**	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Documentation feedback

You can e-mail your comments about product documentation to info@h3c.com.

We appreciate your comments.

Contents

Ethernet OAM commands

display oam

Use **display oam** to display Ethernet OAM connection information.

Syntax

display oam { **local** | **remote** } [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

local: Specifies the local end.

remote: Specifies the remote end.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, the command displays Ethernet OAM connection information for all interfaces.

Examples

Display Ethernet OAM connection information for all local interfaces.

```
<Sysname> display oam local
----------- [GigabitEthernet1/0/1] -----------
 Enable status    : Enable
 Loopback status  : No loopback
 Link status      : UP
 OAM mode         : Active
 PDU              : ANY
 Mux action       : FWD
 Par action       : FWD
```

Display Ethernet OAM connection information for the local interface GigabitEthernet 1/0/1.

```
<Sysname> display oam local interface gigabitethernet 1/0/1
 Enable status    : Enable
 Loopback status  : No loopback
 Link status      : UP
 OAM mode         : Active
 PDU              : ANY
 Mux action       : FWD
 Par action       : FWD
 Flags
   Link fault       : Not occurred
   Dying gasp       : Not occurred
   Critical event   : Not occurred
```

```
  Local evaluating  : COMPLETE
  Remote evaluating : COMPLETE
Packets statistics
  Packet type                    Sent                Received
  ------------------------------------------------------------------
  OAMPDU                         100                 80
  OAMInformation                 64                  60
  OAMEventNotification           36                  20
  OAMUniqueEventNotification     36                  10
  OAMDuplicateEventNotification  0                   10
```

Table 1 Command output

Field	Description
GigabitEthernet1/0/1	Information on GigabitEthernet 1/0/1.
Enable status	Ethernet OAM state: • **Enable**. • **Disable**.
Loopback status	Ethernet OAM loopback state: • **No loopback**—**Remote loopback is disabled**. • **Remote loopback**—**Controlling end of remote loopback**. • **Local loopback**—**Controlled end of remote loopback**.
Link status	Link physical state: • **UP** • **DOWN**.
OAM mode	Local Ethernet OAM mode: • **Active**—The interface operates in active Ethernet OAM mode. • **Passive**—The interface operates in passive Ethernet OAM mode.
PDU	The way in which the local end processes Ethernet OAMPDUs: • **RX_INFO**—The interface receives only Information OAMPDUs and does not send any Ethernet OAMPDUs. • **LF_INFO**—The interface sends only Information OAMPDUs without Information TLV triplets and with their link error flag bits being set. • **INFO**—The interface sends and receives only Information OAMPDUs. • **ANY**—The interface sends and receives Ethernet OAMPDUs of any type.
Mux action	Operating mode of the local transmitter: • **FWD**—The interface can send any packets. • **DISCARD**—The interface only sends Ethernet OAMPDUs.
Par action	Operating mode of the local receiver: • **FWD**—The interface can receive any packets. • **DISCARD**—The interface only receives Ethernet OAMPDUs. • **LB**—The local receiver is in loopback state. All the packets, other than Ethernet OAMPDUs, received on the local receiver are returned to their sources along their original routes.
Flags	Local flags inserted in the local flag fields of the sent Ethernet OAMPDUs.

Field	Description
Link fault	Indicates whether an Ethernet OAM link error is present.
Dying gasp	Indicates whether a fatal error is present.
Critical event	Indicates whether a critical error is present.
Local evaluating	Indicates whether the local-to-remote configuration negotiation is complete: • **COMPLETE**—The negotiation is completed. • **NOTCOMPLETE**—The negotiation is uncompleted.
Remote evaluating	Indicates whether the remote-to-local configuration negotiation is complete: • **COMPLETE**—The negotiation is completed. • **NOTCOMPLETE**—The negotiation is uncompleted. • **RESERVED**—The field is reserved and the negotiation is uncompleted. • **UNSATISFIED**—The remote end is not satisfied with the local configuration and the negotiation is uncompleted.
Packets statistics	Statistics about Ethernet OAMPDUs.
OAMPDU	Total number of sent or received Ethernet OAMPDUs.
OAMInformation	Number of sent or received Information OAMPDUs.
OAMEventNotification	Number of sent or received Event notification OAMPDUs.
OAMUniqueEventNotification	Number of unduplicated sent or received Event notification OAMPDUs.
OAMDuplicateEventNotification	Number of duplicate sent or received Event notification OAMPDUs.

Display Ethernet OAM connection information for all remote interfaces.

```
<Sysname> display oam remote
----------- [GigabitEthernet1/0/1] -----------
 OAM mode         : Active
 MAC address      : 3822-d6a2-a800
 MTU size         : 1500
 Mux action       : FWD
 Par action       : FWD
```

Display Ethernet OAM connection information for the peer interface GigabitEthernet 1/0/1.

```
<Sysname> display oam remote interface gigabitethernet 1/0/1
 OAM mode         : Active
 MAC address      : 3822-d6a2-a800
 MTU size         : 1500
 Mux action       : FWD
 Par action       : FWD
 Configuration
   Unidirectional    : Not supported
   Remote loopback   : Supported
   Link events       : Supported
   MIB retrieval     : Not supported
 Flags
   Link fault        : Not occurred
```

```
Dying gasp       : Not occurred
Critical event   : Not occurred
Local evaluating  : COMPLETE
Remote evaluating : COMPLETE
```

Table 2 Command output

Field	Description
GigabitEthernet1/0/1	Information on GigabitEthernet 1/0/1.
OAM mode	Ethernet OAM mode on the remote end: • **Active**—The interface operates in active Ethernet OAM mode. • **Passive**—The interface operates in passive Ethernet OAM mode.
MAC address	MAC address of the remote end.
MTU size	MTU size, in bytes.
Mux action	Operating mode of the remote transmitter: • **FWD**—The interface can send any packets. • **DISCARD**—The interface only sends Ethernet OAMPDUs.
Par action	Operating mode of the remote receiver: • **FWD**—The interface can receive any packets. • **DISCARD**—The interface only receives Ethernet OAMPDUs. • **LB**—The local receiver is in loopback state. All the packets, other than Ethernet OAMPDUs, received on the local receiver are returned to their sources along their original routes.
Configuration	Configuration of the remote Ethernet OAM entity.
Unidirectional	Indicates whether unidirectional transmission is supported.
Remote loopback	Indicates whether Ethernet OAM remote loopback is supported.
Link events	Indicates whether Ethernet OAM link error events are supported.
MIB retrieval	Indicates whether MIB variable retrieval is supported.
Flags	Values of the peer Ethernet OAM flag fields in OAM packets.
Link fault	Indicates whether an Ethernet OAM link error is present.
Dying gasp	Indicates whether a fatal error is present.
Critical event	Indicates whether a critical error is present.
Local evaluating	Indicates whether the local-to-remote configuration negotiation is complete: • **COMPLETE**—The negotiation is completed. • **NOTCOMPLETE**—The negotiation is uncompleted. • **RESERVED**—The field is reserved and the negotiation is uncompleted. • **UNSATISFIED**—The remote end is not satisfied with the local configuration and the negotiation is uncompleted.
Remote evaluating	Indicates whether the remote-to-local configuration negotiation is complete: • **COMPLETE**—The negotiation is completed. • **NOTCOMPLETE**—The negotiation is uncompleted. • **UNSATISFIED**—The remote end is not satisfied with the local configuration and the negotiation is uncompleted.

Related commands

reset oam

display oam configuration

Use **display oam configuration** to display Ethernet OAM configuration information.

Syntax

display oam configuration [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, the command displays Ethernet OAM configuration globally and for interfaces that do not use the default configuration.

Examples

Display Ethernet OAM configuration globally and for interfaces that do not use the default configuration.

```
<Sysname> display oam configuration
---------------- [Global] ----------------
 OAM timers
   Hello timer       : 1000 milliseconds
   Keepalive timer    : 5000 milliseconds
 Link monitoring
   Errored symbol period
     Window          : 100 x 1000000 symbols
     Threshold       : 1 error symbols
   Errored frame
     Window          : 10 x 100 milliseconds
     Threshold       : 1 error frames
   Errored frame period
     Window          : 1000 x 10000 frames
     Threshold       : 1 error frames
   Errored frame seconds
     Window          : 600 x 100 milliseconds
     Threshold       : 1 error seconds


----------- [GigabitEthernet1/0/1] -----------
 OAM timers
   Hello timer       : 500 milliseconds
   Keepalive timer    : 5000 milliseconds
 Link monitoring
   Errored symbol period
     Window          : 100 x 1000000 symbols
```

```
    Threshold       : 1 error symbols
  Errored frame
    Window          : 10 x 100 milliseconds
    Threshold       : 1 error frames
  Errored frame period
    Window          : 1000 x 10000 frames
    Threshold       : 1 error frames
  Errored frame seconds
    Window          : 600 x 100 milliseconds
    Threshold       : 1 error seconds
```

Table 3 Command output

Field	Description
Global	Global information.
GigabitEthernet1/0/1	Information on GigabitEthernet 1/0/1.
OAM timers	Ethernet OAM connection detection timers.
Hello timer	Ethernet OAM handshake packet transmission interval.
Keepalive timer	Ethernet OAM connection timeout timer.
Link monitoring	Link event detection window and threshold.
Errored symbol period	Errored symbol event.
Errored frame	Errored frame event.
Errored frame period	Errored frame period event.
Errored frame seconds	Errored frame seconds event.
Window	Detection window configured for link events.
Threshold	Triggering threshold configured for link events.

display oam critical-event

Use **display oam critical-event** to display statistics for critical Ethernet OAM link events.

Syntax

display oam critical-event [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, the command displays statistics for the critical Ethernet OAM link events for all interfaces.

Examples

Display statistics for critical Ethernet OAM link events on all interfaces.

```
<Sysname> display oam critical-event
----------- [GigabitEthernet1/0/1] -----------
 Local link status   : UP
 Event statistics
   Link fault       : Not occurred
   Dying gasp       : Not occurred
   Critical event    : Not occurred
```

Table 4 Command output

Field	Description
GigabitEthernet1/0/1	Information on GigabitEthernet 1/0/1.
Local link status	Local link status, up or down.
Event statistics	Statistics for critical Ethernet OAM link events.
Link fault	Indicates whether a link fault is present.
Dying Gasp	Indicates whether a fatal fault is present.
Critical Event	Indicates whether a critical fault is present.

display oam link-event

Use **display oam link-event** to display statistics for Ethernet OAM link error events for local or peer interfaces.

Syntax

display oam link-event { **local** | **remote** } [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

local: Specifies the local end.

remote: Specifies the peer end.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, the command displays statistics for Ethernet OAM link error events for all local or peer interfaces.

Usage guidelines

Ethernet OAM link error events include errored symbol events, errored frame events, errored frame period events, and errored frame seconds events.

Examples

Display statistics for Ethernet OAM link error events for all local interfaces.

```
<Sysname> display oam link-event local
----------- [GigabitEthernet1/0/1] -----------
```

```
 Link status: UP
 OAM local errored symbol event
   Event time stamp       : 35498 x 100 milliseconds
   Errored symbol window    : 100000000 symbols
   Errored symbol threshold : 1 error symbols
   Errored symbol         : 1 error symbols
   Error running total     : 4 error symbols
   Event running total     : 4 events
 OAM local errored frame event
   Event time stamp       : 49582 x 100 milliseconds
   Errored frame window    : 10 x 100 milliseconds
   Errored frame threshold : 1 error frames
   Errored frame         : 1 error frames
   Error running total    : 6 error frames
   Event running total    : 6 events
 OAM local errored frame period event
   Event time stamp             : 16382 x 100 milliseconds
   Errored frame period window    : 10000000 frames
   Errored frame period threshold  : 1 error frames
   Errored frame period          : 1 error frames
   Error running total           : 5 error frames
   Event running total           : 5 events
 OAM local errored frame seconds summary event
   Event time stamp             : 50022 x 100 milliseconds
   Errored frame seconds window    : 600 x 100 milliseconds
   Errored frame seconds threshold : 1 error seconds
   Errored frame seconds         : 1 error seconds
   Error running total           : 1 error seconds
   Event running total           : 1 events
```

Display statistics for Ethernet OAM link error events for all peer interfaces.

```
<Sysname> display oam link-event remote
------------ [GigabitEthernet1/0/1] ------------
 Link status: UP
 OAM remote errored symbol event
   Event time stamp       : 35498 x 100 milliseconds
   Errored symbol window    : 100000000  symbols
   Errored symbol threshold : 1 error symbols
   Errored symbol         : 1 error symbols
   Error running total     : 4 error symbols
   Event running total     : 4 events
 OAM remote errored frame event
   Event time stamp       : 49582 x 100 milliseconds
   Errored frame window    : 10 x 100 milliseconds
   Errored frame threshold : 1 error frames
   Errored frame         : 1 error frames
   Error running total    : 6 error frames
   Event running total    : 6 events
 OAM remote errored frame period event
```

```
  Event time stamp             : 16382 x 100 milliseconds
  Errored frame period window    : 10000000 frames
  Errored frame period threshold  : 1 error frames
  Errored frame period          : 1 error frames
  Error running total           : 5 error frames
  Event running total           : 5 events
OAM remote errored frame seconds summary event
  Event time stamp             : 50022 x 100 milliseconds
  Errored frame seconds window   : 600 x 100 milliseconds
  Errored frame seconds threshold : 1 error seconds
  Errored frame seconds         : 1 error seconds
  Error running total           : 1 error seconds
  Event running total           : 1 events
```

Table 5 Command output

Field	Description
GigabitEthernet1/0/1	Information on GigabitEthernet 1/0/1.
Link status	Link status, up or down.
OAM local/remote errored symbol event	Information about local/remote errored symbol events (available only when remote errored symbol events occur): • **Event time stamp**—Time when an errored symbol event occurred. • **Errored symbol window**—Errored symbol detection interval. • **Errored symbol threshold**—Errored threshold that triggers an errored symbol event. • **Errored symbol**—Number of detected errored symbols in the most recent errored symbol event. • **Error running total**—Total number of errored symbols. • **Event running total**—Total number of errored symbol events that have occurred.
OAM local/remote errored frame event	Information about local/remote end errored frame events (available only when local/remote end errored frame events occur): • **Event time stamp**—Time when an errored frame event occurred. • **Errored frame window**—Errored frame detection interval. • **Errored frame threshold**—Errored threshold that triggers an errored frame event. • **Errored frame**—Number of detected errored frames in the most recent errored frame event. • **Error running total**—Total number of errored frames. • **Event running total**—Total number of errored frame events that have occurred.
OAM local/remote errored frame period event	Information about local or remote errored frame period events (available only when local/remote errored frame period events occur): • **Event time stamp**—Time when an errored frame period event occurred. • **Errored frame period window**—Errored frame period detection interval. • **Errored frame period threshold**—Errored threshold that triggers an errored frame period event. • **Errored frame period**—Number of detected errored frames in the most recent errored frame period event. • **Error running total**—Total number of errored frames that have detected. • **Event running total**—Total number of errored frame period events.

Field	Description
OAM local/remote errored frame seconds summary event	Information about local/remote end errored frame seconds events (available only when local/remote end errored frame seconds events occur): • **Event time stamp**—Time when an errored frame seconds event occurred. • **Errored frame second window**—Errored frame second detection interval. • **Errored Frame seconds threshold**—Errored threshold that triggers an errored frame seconds event. • **Errored frame seconds**—Number of detected errored frame seconds in the most recent errored frame seconds event. • **Error running total**—Total number of errored frame seconds. • **Event running total**—Total number of errored frame seconds events that have occurred.

Related commands

reset oam

oam enable

Use **oam enable** to enable Ethernet OAM.

Use **undo oam enable** to disable Ethernet OAM.

Syntax

oam enable

undo oam enable

Default

Ethernet OAM is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Examples

Enable OAM on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] oam enable
```

oam errored-frame threshold

Use **oam errored-frame threshold** to set the errored frame event triggering threshold for an interface.

Use **undo oam errored-frame threshold** to restore the default.

Syntax

oam errored-frame threshold *threshold-value*

undo oam errored-frame threshold

Default

An interface uses the global setting.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the errored frame event triggering threshold in number of errored frame events, in the range of 0 to 4294967295.

Usage guidelines

The configuration in interface view takes effect only on the specified interface. For an interface, the configuration in interface view takes precedence.

Examples

Set the errored frame event triggering threshold to 100 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] oam errored-frame threshold 100
```

Related commands

display oam configuration

display oam link-event

oam global errored-frame threshold

oam errored-frame window

Use **oam errored-frame window** to set the errored frame event detection window.

Use **undo oam errored-frame window** to restore the default.

Syntax

oam errored-frame window *window-value*

undo oam errored-frame window

Default

An interface uses the global setting.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

window-value: Specifies the errored frame event detection window in the range of 10 to 600, in steps of 10, in 100 milliseconds.

Usage guidelines

The configuration in interface view takes effect only on the specified interface. For an interface, the configuration in interface view takes precedence.

Examples

Set the errored frame event detection window to 2000 milliseconds on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] oam errored-frame window 20
```

Related commands

display oam configuration

display oam link-event

oam global errored-frame window

oam errored-frame-period threshold

Use **oam errored-frame-period threshold** to set the errored frame period event triggering threshold on an interface.

Use **undo oam errored-frame-period threshold** to restore the default.

Syntax

oam errored-frame-period threshold *threshold-value*

undo oam errored-frame-period threshold

Default

An interface uses the global setting.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the errored frame period event triggering threshold in the range of 0 to 4294967295.

Usage guidelines

The configuration in interface view takes effect only on the specified interface. For an interface, the configuration in interface view takes precedence.

Examples

Set the errored frame period event triggering threshold to 100 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] oam errored-frame-period threshold 100
```

Related commands

display oam configuration

display oam link-event

oam global errored-frame-period threshold

oam errored-frame-period window

Use **oam errored-frame-period window** to set the errored frame period event detection window.

Use **undo oam errored-frame-period window** to restore the default.

Syntax

oam errored-frame-period window *window-value*

undo oam errored-frame-period window

Default

An interface uses the global setting.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

window-value: Specifies the errored frame period event detection window in the range of 1 to 65535. The value of this argument must be a multiple of 10000.

Usage guidelines

The configuration in interface view takes effect only on the specified interface. For an interface, the configuration in interface view takes precedence.

Examples

Set the errored frame period event detection window to 20000000 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] oam errored-frame-period window 2000
```

Related commands

display oam configuration

display oam link-event

oam global errored-frame-period window

oam errored-frame-seconds threshold

Use **oam errored-frame-seconds threshold** to set the errored frame seconds event triggering threshold on an interface.

Use **undo oam errored-frame-seconds threshold** to restore the default.

Syntax

oam errored-frame-seconds threshold *threshold-value*

undo oam errored-frame-seconds threshold

Default

An interface uses the global setting.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the errored frame seconds event triggering threshold in the range of 0 to 900.

Usage guidelines

The value of the errored frame seconds event triggering threshold cannot be greater than the value of the errored frame seconds event detection window (in seconds). Otherwise, errored frame seconds events cannot be generated.

The configuration in interface view takes effect only on the specified interface. For an interface, the configuration in interface view takes precedence.

Examples

Set the errored frame seconds event triggering threshold to 100 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] oam errored-frame-seconds threshold 100
```

Related commands

display oam configuration

display oam link-event

oam errored-frame-seconds window

oam global errored-frame-seconds threshold

oam errored-frame-seconds window

Use **oam errored-frame-seconds window** to set the errored frame seconds event detection window.

Use **undo oam errored-frame-seconds window** to restore the default.

Syntax

oam errored-frame-seconds window *window-value*

undo oam errored-frame-seconds window

Default

An interface uses the global setting.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

window-value: Specifies the errored frame seconds event detection window in the range of 100 to 9000, in steps of 10, in 100 milliseconds.

Usage guidelines

The value of the errored frame seconds event triggering threshold cannot be greater than the value of the errored frame seconds event detection window (in seconds). Otherwise, errored frame seconds events cannot be generated.

The configuration in interface view takes effect only on the specified interface. For an interface, the configuration in interface view takes precedence.

Examples

Set the errored frame seconds event detection window to 10000 milliseconds on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] oam errored-frame-seconds window 100
```

Related commands

display oam configuration

display oam link-event

oam errored-frame-seconds threshold

oam errored-frame-seconds period

oam errored-symbol-period threshold

Use **oam errored-symbol-period threshold** to set the errored symbol event triggering threshold.

Use **undo oam errored-symbol-period threshold** to restore the default.

Syntax

oam errored-symbol-period threshold *threshold-value*

undo oam errored-symbol-period threshold

Default

An interface uses the global setting.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the errored symbol event triggering threshold in the range of 0 to 4294967295.

Usage guidelines

The configuration in interface view takes effect only on the specified interface. For an interface, the configuration in interface view takes precedence.

Examples

Set the errored symbol event triggering threshold to 100 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] oam errored-symbol-period threshold 100
```

Related commands

display oam configuration

display oam link-event

oam global errored-symbol-period threshold

oam errored-symbol-period window

Use **oam errored-symbol-period window** to set the errored symbol event detection window.

Use **undo oam errored-symbol-period window** to restore the default.

Syntax

oam errored-symbol-period window *window-value*

undo oam errored-symbol-period window

Default

An interface uses the global setting.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

window-value: Specifies the errored symbol event detection window in the range of 1 to 65535. The actual value is the value of this argument multiplied by 1000000.

Usage guidelines

The configuration in interface view takes effect only on the specified interface. For an interface, the configuration in interface view takes precedence.

Examples

Set the errored symbol event detection window to 200000000 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] oam errored-symbol-period window 200
```

Related commands

display oam configuration

display oam link-event

oam global errored-symbol-period window

oam global errored-frame threshold

Use **oam global errored-frame threshold** to set the global errored frame event triggering threshold.

Use **undo oam global errored-frame threshold** to restore the default.

Syntax

oam global errored-frame threshold *threshold-value*

undo oam global errored-frame threshold

Default

The errored frame event triggering threshold is 1.

Views

System view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the errored frame event triggering threshold in the range of 0 to 4294967295.

Usage guidelines

The configuration in system view takes effect on all interfaces, but has a lower precedence than the configuration in interface view.

Examples

Set the errored frame event triggering threshold to 100.

```
<Sysname> system-view
[Sysname] oam global errored-frame threshold 100
```

Related commands

display oam configuration

display oam link-event

oam errored-frame threshold

oam global errored-frame window

Use **oam global errored-frame window** to set the global errored frame event detection window.

Use **undo oam global errored-frame window** to restore the default.

Syntax

oam global errored-frame window *window-value*

undo oam global errored-frame window

Default

The global errored frame event detection window is 1000 milliseconds.

Views

System view

Predefined user roles

network-admin

Parameters

window-value: Specifies the errored frame event detection window in the range of 10 to 600, in steps of 10, in 100 milliseconds.

Usage guidelines

The configuration in system view takes effect on all interfaces, but has a lower precedence than the configuration in interface view.

Examples

Set the errored frame event detection window to 2000 milliseconds.

```
<Sysname> system-view
[Sysname] oam global errored-frame window 20
```

Related commands

display oam configuration

display oam link-event

oam errored-frame window

oam global errored-frame-period threshold

Use **oam global errored-frame-period threshold** to set the global errored frame period event triggering threshold.

Use **undo oam global errored-frame-period threshold** to restore the default.

Syntax

oam global errored-frame-period threshold *threshold-value*

undo oam global errored-frame-period threshold

Default

The errored frame period event triggering threshold is 1.

Views

System view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the errored frame period event triggering threshold in the range of 0 to 4294967295.

Usage guidelines

The configuration in system view takes effect on all interfaces, but has a lower precedence than the configuration in interface view.

Examples

Set the errored frame period event triggering threshold to 100.

```
<Sysname> system-view
[Sysname] oam global errored-frame-period threshold 100
```

Related commands

display oam configuration

display oam link-event

oam errored-frame-period threshold

oam global errored-frame-period window

Use **oam global errored-frame-period window** to set the global errored frame period event detection window.

Use **undo oam global errored-frame-period window** to restore the default.

Syntax

oam global errored-frame-period window *window-value*

undo oam global errored-frame-period window

Default

The global errored frame period event detection window is 10000000.

Views

System view

Predefined user roles

network-admin

Parameters

window-value: Specifies the errored frame period event detection window in the range of 1 to 65535. The value of this argument must be a multiple of 10000.

Usage guidelines

The configuration in system view takes effect on all interfaces, but has a lower precedence than the configuration in interface view.

Examples

Set the errored frame period event detection window to 20000000.

```
<Sysname> system-view
[Sysname] oam global errored-frame-period window 2000
```

Related commands

display oam configuration

display oam link-event

oam errored-frame-period window

oam global errored-frame-seconds threshold

Use **oam global errored-frame-seconds threshold** to set the global errored frame seconds event triggering threshold.

Use **undo oam global errored-frame-seconds threshold** to restore the default.

Syntax

oam global errored-frame-seconds threshold *threshold-value*

undo oam global errored-frame-seconds threshold

Default

The global errored frame seconds event detection interval is 1.

Views

System view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the errored frame seconds event triggering threshold in the range of 0 to 900.

Usage guidelines

The value of the errored frame seconds event triggering threshold cannot be greater than the value of the errored frame seconds event detection window (in seconds). Otherwise, errored frame seconds events cannot be generated.

The configuration in system view takes effect on all interfaces, but has a lower precedence than the configuration in interface view.

Examples

Set the errored frame seconds event triggering threshold to 100.

```
<Sysname> system-view
[Sysname] oam global errored-frame-seconds threshold 100
```

Related commands

display oam configuration

display oam link-event

oam errored-frame-seconds threshold

oam global errored-frame-seconds window

oam global errored-frame-seconds window

Use **oam global errored-frame-seconds window** to set the global errored frame seconds event detection window.

Use **undo oam global errored-frame-seconds window** to restore the default.

Syntax

oam global errored-frame-seconds window *window-value*

undo oam global errored-frame-seconds window

Default

The global errored frame seconds event detection window is 60000 milliseconds.

Views

System view

Predefined user roles

network-admin

Parameters

window-value: Specifies the errored frame seconds event detection window in the range of 100 to 9000, in steps of 10, in 100 milliseconds.

Usage guidelines

The value of the errored frame seconds event triggering threshold cannot be greater than the value of the errored frame seconds event detection window (in seconds). Otherwise, errored frame seconds events cannot be generated.

The configuration in system view takes effect on all interfaces, but has a lower precedence than the configuration in interface view.

Examples

Set the errored frame seconds event detection window to 10000 milliseconds.

```
<Sysname> system-view
[Sysname] oam global errored-frame-seconds window 100
```

Related commands

display oam configuration

display oam link-event

oam errored-frame-seconds period

oam global errored-frame-seconds threshold

oam global errored-symbol-period threshold

Use **oam global errored-symbol-period threshold** to set the global errored symbol event triggering threshold.

Use **undo oam global errored-symbol-period threshold** to restore the default.

Syntax

oam global errored-symbol-period threshold *threshold-value*

undo oam global errored-symbol-period threshold

Default

The global errored symbol event triggering threshold is 1.

Views

System view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the errored symbol event triggering threshold in the range of 0 to 4294967295.

Usage guidelines

The configuration in system view takes effect on all interfaces, but has a lower precedence than the configuration in interface view.

Examples

Set the errored symbol event triggering threshold to 100.

```
<Sysname> system-view
[Sysname] oam global errored-symbol-period threshold 100
```

Related commands

display oam configuration

display oam link-event

oam errored-symbol-period threshold

oam global errored-symbol-period window

Use **oam global errored-symbol-period window** to set the global errored symbol event detection window.

Use **undo oam global errored-symbol-period window** to restore the default.

Syntax

oam global errored-symbol-period window *window-value*

undo oam global errored-symbol-period window

Default

The global errored symbol event detection window is 100000000.

Views

System view

Predefined user roles

network-admin

Parameters

window-value: Specifies the errored symbol event detection window in the range of 1 to 65535. The value of this argument must be a multiple of 1000000.

Usage guidelines

The configuration in system view takes effect on all interfaces, but has a lower precedence than the configuration in interface view.

Examples

Set the errored symbol event detection window to 200000000.

```
<Sysname> system-view
[Sysname] oam global errored-symbol-period window 200
```

Related commands

display oam configuration

display oam link-event

oam global errored-symbol-period window

oam global timer hello

Use **oam global timer hello** to configure the global Ethernet OAM handshake packet transmission interval.

Use **undo oam global timer hello** to restore the default.

Syntax

oam global timer hello *interval*

undo oam global timer hello

Default

The global Ethernet OAM handshake packet transmission interval is 1000 milliseconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the Ethernet OAM handshake packet transmission interval, in steps of 100, in milliseconds. The value range for the *interval* argument is 500 to 5000.

Usage guidelines

After the timeout timer of an Ethernet OAM connection expires, the local OAM entity ages out and terminates its connection with the peer OAM entity. To keep the Ethernet OAM connections stable, set the connection timeout timer to be a minimum of five times the handshake packet transmission interval.

The configuration in system view takes effect on all interfaces, but has a lower precedence than the configuration in interface view.

Examples

Set the Ethernet OAM handshake packet transmission interval to 600 milliseconds.

```
<Sysname> system-view
[Sysname] oam global timer hello 600
```

Related commands

display oam configuration

oam timer hello

oam global timer keepalive

Use **oam global timer keepalive** to configure the global Ethernet OAM connection timeout timer.

Use **undo oam global timer keepalive** to restore the default.

Syntax

oam global timer keepalive *interval*

undo oam global timer keepalive

Default

The global Ethernet OAM connection timeout timer is 5000 milliseconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the Ethernet OAM connection timeout timer, in steps of 100, in milliseconds. The value range for the *interval* argument is 1000 to 25000.

Usage guidelines

After the timeout timer of an Ethernet OAM connection expires, the local OAM entity ages out and terminates its connection with the peer OAM entity. To keep the Ethernet OAM connections stable, set the connection timeout timer to be a minimum of five times the handshake packet transmission interval.

The configuration in system view takes effect on all interfaces, but has a lower precedence than the configuration in interface view.

Examples

Set the Ethernet OAM connection timeout timer to 6000 milliseconds.

```
<Sysname> system-view
[Sysname] oam global timer keepalive 6000
```

Related commands

display oam configuration

oam timer keepalive

oam mode

Use **oam mode** to set the Ethernet OAM mode.

Use **undo oam mode** to restore the default.

Syntax

oam mode { **active** | **passive** }

undo oam mode

Default

An Ethernet OAM-enabled Ethernet interface operates in active Ethernet OAM mode.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

active: Specifies the active Ethernet OAM mode.

passive: Specifies the passive Ethernet OAM mode.

Usage guidelines

To change the Ethernet OAM mode of an Ethernet OAM-enabled Ethernet interface, first disable Ethernet OAM on the interface.

Examples

Disable Ethernet OAM on GigabitEthernet 1/0/1, and then configure GigabitEthernet 1/0/1 to operate in passive Ethernet OAM mode.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo oam enable
[Sysname-GigabitEthernet1/0/1] oam mode passive
```

Related commands

oam enable

oam remote-failure action

Use **oam remote-failure action** to configure the action an interface takes after it receives an Ethernet OAM event from the remote end.

Use **undo oam remote-failure action** to remove the configuration.

Syntax

oam remote-failure { **connection-expired** | **critical-event** | **dying-gasp** | **link-fault** } **action error-link-down**

undo oam remote-failure { **connection-expired** | **critical-event** | **dying-gasp** | **link-fault** } **action error-link-down**

Default

An interface only logs the Ethernet OAM event it receives from the remote end.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

connection-expired: Specifies a connection timeout event.

critical-event: Specifies a critical event.

dying-gasp: Specifies a fatal event.

link-fault: Specifies a link fault event.

error-link-down: Terminates the OAM connection, and sets the link state of the interface to down.

Examples

Configure GigabitEthernet 1/0/1 to terminate the OAM connection after it receives a critical event from the remote end, and set the link state of the interface to down.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] oam remote-failure critical-event action error-link-down
```

oam remote-loopback

Use **oam remote-loopback start** to enable Ethernet OAM remote loopback on an interface.

Use **oam remote-loopback stop** to disable Ethernet OAM remote loopback on an interface.

Syntax

oam remote-loopback start

oam remote-loopback stop

Default

Ethernet OAM remote loopback is disabled on an interface.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

Ethernet OAM remote loopback is available only after the Ethernet OAM connection is established. It can be performed only by the Ethernet OAM entities operating in active Ethernet OAM mode.

You can enable Ethernet OAM remote loopback on a specified interface in user view or system view. You can also enable it on the current interface in interface view. The configurations have the same effect.

Examples

Configure active Ethernet OAM mode and enable Ethernet OAM on GigabitEthernet 1/0/1. Enable Ethernet OAM remote loopback on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] oam mode active
[Sysname-GigabitEthernet1/0/1] oam enable
[Sysname-GigabitEthernet1/0/1] oam remote-loopback start
```

Related commands

oam enable

oam mode

oam remote-loopback interface

oam remote-loopback interface

Use **oam remote-loopback start interface** to enable Ethernet OAM remote loopback on an interface.

Use **oam remote-loopback stop interface** to disable Ethernet OAM remote loopback on an interface.

Syntax

oam remote-loopback start interface *interface-type interface-number*

oam remote-loopback stop interface *interface-type interface-number*

Default

Ethernet OAM remote loopback is disabled on an interface.

Views

User view

System view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

Ethernet OAM remote loopback is available only after the Ethernet OAM connection is established. It can be performed only by the Ethernet OAM entities operating in active Ethernet OAM mode.

You can enable Ethernet OAM remote loopback on a specified interface in user view or system view. You can also enable it on the current interface in interface view. The configurations have the same effect.

Examples

Configure the active Ethernet OAM mode and enable Ethernet OAM on GigabitEthernet 1/0/1. Enable Ethernet OAM remote loopback on GigabitEthernet 1/0/1 in system view.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] oam mode active
[Sysname-GigabitEthernet1/0/1] oam enable
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] oam remote-loopback start interface gigabitethernet 1/0/1
```

Related commands

oam enable

oam mode

oam remote-loopback

oam remote-loopback reject-request

Use **oam remote-loopback reject-request** to configure an interface to reject the Ethernet OAM remote loopback request from a remote interface.

Use **undo oam remote-loopback reject-request** to restore the default.

Syntax

oam remote-loopback reject-request

undo oam remote-loopback reject-request

Default

An interface does not reject the Ethernet OAM remote loopback request from a remote interface.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

If an interface is in loopback state when you execute the **oam remote-loopback reject-request** command, the configuration takes effect when the next loopback starts.

Examples

Configure GigabitEthernet 1/0/1 to reject the Ethernet OAM remote loopback request from a remote interface.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] oam remote-loopback reject-request
```

oam timer hello

Use **oam timer hello** to configure the Ethernet OAM handshake packet transmission interval.

Use **undo oam timer hello** to restore the default.

Syntax

oam timer hello *interval*

undo oam timer hello

Default

An interface uses the global setting.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

interval: Specifies the Ethernet OAM handshake packet transmission interval, in steps of 100, in milliseconds. The value range for the *interval* argument is 500 to 5000.

Usage guidelines

After the timeout timer of an Ethernet OAM connection expires, the local OAM entity ages out and terminates its connection with the peer OAM entity. To keep the Ethernet OAM connections stable, set the connection timeout timer to be at least five times the handshake packet transmission interval.

The configuration in interface view takes effect only on the specified interface. For an interface, the configuration in interface view takes precedence.

Examples

Set the Ethernet OAM handshake packet transmission interval to 600 milliseconds on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] oam timer hello 600
```

Related commands

display oam configuration

oam global timer hello

oam timer keepalive

Use **oam timer keepalive** to configure the Ethernet OAM connection timeout timer.

Use **undo oam timer keepalive** to restore the default.

Syntax

oam timer keepalive *interval*

undo oam timer keepalive

Default

An interface uses the global setting.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

interval: Specifies the Ethernet OAM connection timeout timer, in steps of 100, in milliseconds. The value range for the *interval* argument is 1000 to 25000.

Usage guidelines

After the timeout timer of an Ethernet OAM connection expires, the local OAM entity ages out and terminates its connection with the peer OAM entity. To keep the Ethernet OAM connections stable, set the connection timeout timer to be a minimum of five times the handshake packet transmission interval.

The configuration in interface view takes effect only on the specified interface. For an interface, the configuration in interface view takes precedence.

Examples

Set the Ethernet OAM connection timeout timer to 6000 milliseconds on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] oam timer keepalive 6000
```

Related commands

display oam configuration

oam global timer keepalive

reset oam

Use **reset oam** to clear statistics for Ethernet OAM packets and Ethernet OAM link error events.

Syntax

reset oam [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, the command clears statistics for Ethernet OAM packets and Ethernet OAM link error events for all interfaces.

Examples

Clear statistics for Ethernet OAM packets and Ethernet OAM link error events for all interfaces.

```
<Sysname> reset oam
```

Related commands

display oam

display oam link-event

Contents

CFD commands

cfd ais enable

Use **cfd ais enable** to enable AIS.

Use **undo cfd ais enable** to disable AIS.

Syntax

cfd ais enable

undo cfd ais enable

Default

AIS is disabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable AIS.

```
<Sysname> system-view
[Sysname] cfd ais enable
```

Related commands

cfd ais level

cfd ais period

cfd ais level

Use **cfd ais level** to configure the AIS frame transmission level.

Use **undo cfd ais level** to remove the AIS frame transmission level.

Syntax

cfd ais level *level-value* **service-instance** *instance-id*

undo cfd ais level *level-value* **service-instance** *instance-id*

Default

The AIS frame transmission level is not configured.

Views

System view

Predefined user roles

network-admin

Parameters

level *level-value*: Specifies the AIS frame transmission level in the range of 1 to 7.

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767.

Usage guidelines

If no AIS frame transmission level is configured for a service instance, the MEPs in the service instance cannot send AIS frames.

The AIS frame transmission level must be higher than the MD level of the service instance.

Examples

Configure the AIS frame transmission level as 3 in service instance 1.

```
<Sysname> system-view
[Sysname] cfd ais level 3 service-instance 1
```

Related commands

cfd ais enable

cfd ais period

cfd ais period

Use **cfd ais period** to configure the AIS frame transmission period.

Use **undo cfd ais period** to remove the AIS frame transmission period.

Syntax

cfd ais period *period-value* **service-instance** *instance-id*

undo cfd ais period *period-value* **service-instance** *instance-id*

Default

The AIS frame transmission period is 1 second.

Views

System view

Predefined user roles

network-admin

Parameters

period *period-value*: Specifies the AIS frame transmission period in the range of 1 to 60 seconds.

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767.

Examples

Configure the AIS frame transmission period as 60 seconds in service instance 1.

```
<Sysname> system-view
[Sysname] cfd ais period 60 service-instance 1
```

Related commands

cfd ais enable

cfd ais level

cfd ais-track link-status global

Use **cfd ais-track link-status global** to enable port status-AIS collaboration.

Use **undo cfd ais-track link-status global** to disable port status-AIS collaboration.

Syntax

cfd ais-track link-status global

undo cfd ais-track link-status global

Default

Port status-AIS collaboration is disabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable port status-AIS collaboration.

```
<Sysname> system-view
[Sysname] cfd ais-track link-status global
```

Related commands

cfd ais-track link-status level

cfd ais-track link-status period

cfd ais-track link-status vlan

cfd ais-track link-status level

Use **cfd ais-track link-status level** to configure the EAIS frame transmission level.

Use **undo cfd ais-track link-status level** to restore the default.

Syntax

cfd ais-track link-status level *level-value*

undo cfd ais-track link-status level

Default

The EAIS frame transmission level is not configured.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

level *level-value*: Specifies the EAIS frame transmission level in the range of 0 to 7.

Usage guidelines

If no EAIS frame transmission level is configured on a port, the port cannot send EAIS frames.

Follow these guidelines when you use the command:

- Configurations in Ethernet interface view take effect only on the current interface.
- Configurations in aggregate interface view take effect only on the current aggregate interface.
- Configurations on a member port take effect only when the member port leaves the aggregation group.

Examples

Configure the EAIS frame transmission level as 3 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] cfd ais-track link-status level 3
```

Related commands

cfd ais-track link-status global

cfd ais-track link-status period

cfd ais-track link-status vlan

cfd ais-track link-status period

Use **cfd ais-track link-status period** to configure the EAIS frame transmission period.

Use **undo cfd ais-track link-status period** to restore the default.

Syntax

cfd ais-track link-status period *period-value*

undo cfd ais-track link-status period

Default

The EAIS frame transmission period is not configured.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

period *period-value*: Specifies the EAIS frame transmission period in the range of 1 to 60 seconds.

Usage guidelines

If no EAIS frame transmission period is configured on a port, the port cannot send EAIS frames.

Follow these guidelines when you use the command:

- Configurations in Ethernet interface view take effect only on the current interface.
- Configurations in aggregate interface view take effect only on the current aggregate interface.
- Configurations on a member port take effect only when the member port leaves the aggregation group.

Examples

Configure the EAIS frame transmission period as 60 seconds on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] cfd ais-track link-status period 60
```

Related commands

cfd ais-track link-status global

cfd ais-track link-status level

cfd ais-track link-status vlan

cfd ais-track link-status vlan

Use **cfd ais-track link-status vlan** to specify the VLANs where the EAIS frames can be transmitted.

Use **undo cfd ais-track link-status vlan** to remove the VLANs where the EAIS frames can be transmitted.

Syntax

cfd ais-track link-status vlan *vlan-list*

undo cfd ais-track link-status vlan *vlan-list*

Default

The EAIS frames can be transmitted only within the default VLAN of the port.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies the VLANs where the EAIS frames can be transmitted. The *vlan-list* argument specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN ID or a range of VLAN IDs in the form of *vlan-id* [**to** *vlan-id*]. The value range for VLAN IDs is 1 to 4094.

Usage guidelines

The EAIS frames are transmitted within the intersection of the VLANs specified with this command and the existing VLANs on the device.

If the command is executed multiple times, the combination of the VLANs specified in each command takes effect.

Follow these guidelines when you use the command:

- Configurations in Ethernet interface view take effect only on the current interface.
- Configurations in aggregate interface view take effect only on the current aggregate interface.
- Configurations on a member port take effect only when the member port leaves the aggregation group.

Examples

On port GigabitEthernet 1/0/1, specify VLANs 100 through 200 as the VLANs where the EAIS frames can be transmitted.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] cfd ais-track link-status vlan 100 to 200
```

Related commands

cfd ais-track link-status global

cfd ais-track link-status level

cfd ais-track link-status period

cfd cc enable

Use **cfd cc enable** to enable CCM sending on a specified MEP.

Use **undo cfd cc enable** to disable CCM sending on a specified MEP.

Syntax

cfd cc service-instance *instance-id* **mep** *mep-id* **enable**

undo cfd cc service-instance *instance-id* **mep** *mep-id* **enable**

Default

The CCM sending feature is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767.

mep *mep-id*: Specifies a MEP by its ID in the range of 1 to 8191.

Usage guidelines

Follow these guidelines when you use the command:

- Configurations in Ethernet interface view take effect only on the current interface.
- Configurations in aggregate interface view take effect only on the current aggregate interface.
- If the MEP belongs to an MA that does not carry the VLAN attribute, configurations on a member port of an aggregation group view take effect only on the current member port.
- If the MEP belongs to an MA that carries the VLAN attribute, configurations on a member port of an aggregation group take effect only when the member port leaves the aggregation group.

Examples

On port GigabitEthernet 1/0/1, enable CCM sending on MEP 3 in service instance 5.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] cfd cc service-instance 5 mep 3 enable
```

Related commands

cfd cc interval

cfd cc interval

Use **cfd cc interval** to set the value of the interval field in the CCM messages.

Use **undo cfd cc interval** to remove the value of the interval field in the CCM messages.

Syntax

cfd cc interval *interval-value* **service-instance** *instance-id*

undo cfd cc interval [*interval-value*] **service-instance** *instance-id*

Default

The value of this field is 4 for all CCM messages sent.

Views

System view

Predefined user roles

network-admin

Parameters

interval *interval-value*: Specifies the value of the interval field in CCM messages. The value range for the interval field is 1 to 7. If you set the value to 1 or 2, the continuity check might work incorrectly due to hardware restrictions.

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767.

Usage guidelines

When setting the CCM interval, use the settings described in Table 1.

Table 1 CCM interval field encoding

CCM interval field	Transmission interval	Maximum CCM lifetime
1	10/3 milliseconds	35/3 milliseconds
2	10 milliseconds	35 milliseconds
3	100 milliseconds	350 milliseconds
4	1 second	3.5 seconds
5	10 seconds	35 seconds
6	60 seconds	210 seconds
7	600 seconds	2100 seconds

Examples

Set the value of the interval field to 3 in CCM messages sent by MEPs in service instance 2.

```
<Sysname> system-view
[Sysname] cfd cc interval 3 service-instance 2
```

Related commands

cfd cc enable

cfd dm one-way

Use **cfd dm one-way** to enable one-way delay measurement (DM).

Syntax

cfd dm one-way service-instance *instance-id* **mep** *mep-id* { **target-mac** *mac-address* | **target-mep** *target-mep-id* } [**number** *number*]

Views

Any view

Predefined user roles

network-admin

Parameters

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767.

mep *mep-id*: Specifies the source MEP by its ID in the range of 1 to 8191.

target-mac *mac-address*: Specifies the target MEP by its MAC address in the format of H-H-H.

target-mep *target-mep-id*: Specifies the target MEP by its ID in the range of 1 to 8191.

number *number*: Specifies the number of 1DM frames sent. The value range for the *number* argument is 2 to 10, and the default is 5.

Usage guidelines

The one-way DM function measures the one-way frame delay between the source and target MEPs by using 1DM frames.

To view the one-way delay test result, use the **display cfd dm one-way history** command on the target MEP.

Examples

Enable the one-way DM function to test the one-way frame delay from source MEP 1101 to target MEP 1003 in service instance 1.

```
<Sysname> cfd dm one-way service-instance 1 mep 1101 target-mep 1003
5 1DMs have been sent. Please check the result on the remote device.
```

Related commands

display cfd dm one-way history

reset cfd dm one-way history

cfd dm two-way

Use **cfd dm two-way** to enable two-way DM.

Syntax

cfd dm two-way service-instance *instance-id* **mep** *mep-id* { **target-mac** *mac-address* | **target-mep** *target-mep-id* } [**dot1p** *dot1p-value*] [**number** *number*] [**interval** *interval*]

Views

Any view

Predefined user roles

network-admin

Parameters

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767.

mep *mep-id*: Specifies the source MEP by its ID in the range of 1 to 8191.

target-mac *mac-address*: Specifies the target MEP by its MAC address, which is in the format of H-H-H.

target-mep *target-mep-id*: Specifies the target MEP by its ID in the range of 1 to 8191.

dot1p *dot1p-value*: Specifies an 802.1p priority for DMM frames. The value range for the *dot1p-value* argument is 0 to 7. The default value is 7.

number *number*: Specifies the number of DMM frames to be sent. The value range for the *number* argument is 2 to 10, and the default is 5.

interval*interval*: Specifies the DMM frame sending interval, in seconds. The value takes 1 or 10. The default value is 1.

Usage guidelines

The two-way DM function measures the two-way frame delay between the source and target MEPs by using DMM frames and DMR frames.

Examples

Enable the two-way DM function to test the two-way frame delay between source MEP 1101 and target MEP 2001 in service instance 1.

```
<Sysname> cfd dm two-way service-instance 1 mep 1101 target-mep 2001
Frame delay:
Reply from 0010-fc00-6512: 2406us
Reply from 0010-fc00-6512: 2215us
Reply from 0010-fc00-6512: 2112us
Reply from 0010-fc00-6512: 1812us
Reply from 0010-fc00-6512: 2249us
Average: 2158us
Sent DMMs: 5        Received: 5        Lost: 0

Frame delay variation: 191us 103us 300us 437us
Average: 257us
```

Table 2 Command output

Field	Description
Reply from 0010-fc00-6512	Delay of the DMR frames returned from the MEP with MAC address 0010-FC00-6512.
Average	Average frame delay or average frame delay variation.
Sent DMMs	Number of sent DMM frames .
Received	Number of received DMR frames.
Lost	Number of lost DMM frames.

cfd enable

Use **cfd enable** to enable CFD.

Use **undo cfd enable** to disable CFD.

Syntax

cfd enable

undo cfd enable

Default

CFD is disabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable CFD.

```
<Sysname> system-view
[Sysname] cfd enable
```

cfd linktrace

Use **cfd linktrace** to identify the path between the source MEP and target MP.

Syntax

cfd linktrace service-instance *instance-id* **mep** *mep-id* { **target-mac** *mac-address* | **target-mep** *target-mep-id* } [**ttl** *ttl-value*] [**hw-only**]

Views

Any view

Predefined user roles

network-admin

Parameters

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767.

mep *mep-id*: Specifies the source MEP by its ID in the range of 1 to 8191.

target-mac *mac-address*: Specifies the destination MAC address, in the format of H-H-H.

target-map *target-mep-id*: Specifies the destination MEP by its ID in the range of 1 to 8191.

ttl *ttl-value*: Specifies the TTL value in the range of 1 to 255. The default value is 64.

hw-only: Sets the hw-only bits of the LTMs sent. If you specify this keyword, the MIP does not flood LTMs that have an unknown destination MAC address.

Usage guidelines

This command identifies the path between the source MEP and target MP by using LTMs and LTRs.

Examples

Identify the path between source MEP 1101 and target MEP 2001 in service instance 1.

```
<Sysname> cfd linktrace service-instance 1 mep 1101 target-mep 2001
Linktrace to MEP 2001 with the sequence number 1101-43361:
MAC address               TTL     Last MAC         Relay action
0010-fc00-6512            63      0010-fc00-6500   Hit
```

Table 3 Command output

Field	Description
Linktrace to MEP 2001 with the sequence number 1101-43361	Linktrace to target MEP 2001 with the sequence number 1101-43361.
MAC address	Source MAC address in the LTRs.
TTL	TTL of the LTM when it passes the device.
Last MAC	MAC address of the last-hop device the LTM passes.
Relay action	Indicates whether the forwarding device found the destination MAC address in its MAC address table. When the standard version (IEEE 802.1ag) of CFD is used: • **Hit**—The current device is the destination device. • **FDB**—The forwarding device found the destination MAC address. • **MPDB**—The destination MAC address is not found, or the destination MAC address is found in the MEP or MIP database.

Related commands

cfd linktrace auto-detection

display cfd linktrace-reply

cfd linktrace auto-detection

Use **cfd linktrace auto-detection** to enable automatic sending of LTMs.

Use **undo cfd linktrace auto-detection** to disable automatic sending of LTMs.

Syntax

cfd linktrace auto-detection [**size** *size-value*]

undo cfd linktrace auto-detection

Default

Automatic sending of LTMs is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

size *size-value*: Specifies the size of the buffer used to store the auto-detection result, in the range of 1 to 100 (in terms of auto-detection times). The default value is 5, which means the buffer stores the results of the recent five auto-detections.

Usage guidelines

This command enables the source MEP to send LTMs when it fails to receive CCMs from the target MEP within 3.5 times the sending interval. The destination of the LTMs is the target MEP, and the TTL field value is 255. Based on the returned LTRs, the fault source can be located on the faulty link.

If you disable automatic LTM sending, the content stored in the buffer will be removed.

Examples

Enable automatic LTM sending, and set the size of the buffer used to store the auto-detection result to 100 (in terms of auto-detection times).

```
<Sysname> system-view
[Sysname] cfd linktrace auto-detection size 100
```

Related commands

cfd linktrace

display cfd linktrace-reply auto-detection

cfd loopback

Use **cfd loopback** to enable loopback (LB).

Syntax

cfd loopback service-instance *instance-id* **mep** *mep-id* { **target-mac** *mac-address* | **target-mep** *target-mep-id* } [**number** *number*]

Views

Any view

Predefined user roles

network-admin

Parameters

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767.

mep *mep-id*: Specifies the source MEP by its ID in the range of 1 to 8191.

target-mac *mac-address*: Specifies the destination MAC address of the MP, in the format of H-H-H.

target-mep *target-mep-id*: Specifies the target MEP by its ID in the range of 1 to 8191.

number *number*: Specifies the number of the sent LBMs packets. The value is in the range of 1 to 10. The default value is 5.

Usage guidelines

The LB function verifies link connectivity between the source MEP and the target MP by using LBMs and LBRs.

Examples

Enable LB for the link between MEP 1101 and MEP 2001 in service instance 1 (assume that the link status is normal).

```
<Sysname> cfd loopback service-instance 1 mep 1101 target-mep 2001
Loopback to MEP 2001 with the sequence number start from 1101-43404:
Reply from 0010-fc00-6512: sequence number=1101-43404 Time=5ms
Reply from 0010-fc00-6512: sequence number=1101-43405 Time=5ms
```

```
Reply from 0010-fc00-6512: sequence number=1101-43406 Time=5ms
Reply from 0010-fc00-6512: sequence number=1101-43407 Time=5ms
Reply from 0010-fc00-6512: sequence number=1101-43408 Time=5ms
Sent: 5        Received: 5        Lost: 0
```

Enable LB for the link between MEP 1101 and MEP 2001 in service instance 1 (assume that the link status is abnormal).

```
<Sysname> cfd loopback service-instance 1 mep 1101 target-mep 2001
Loopback to MEP 2001 with the sequence number start from 1101-43404:
Sent: 5        Received: 0        Lost: 5
```

Table 4 Command output

Field	Description
Loopback to MEP 2001 with the sequence number start from 1101-43404	Sends LBMs to remote MEP 2001 with the sequence number starting with 1101-43404.
Reply from 0010-fc00-6512	Reply from the MP with the MAC address 0010-FC00-6512.
sequence number	Sequence number in the LBR messages.
Time=5ms	The interval between the sending of LBMs and receiving of LBRs is 5 milliseconds.
Sent	Number of sent LBMs.
Received	Number of received LBRs.
Lost	Number of lost LBRs.

cfd md

Use **cfd md** to create an MD.

Use **undo cfd md** to delete an MD.

Syntax

cfd md *md-name* [**index** *index-value*] **level** *level-value* [**md-id** { **dns** *dns-name* | **mac** *mac-address subnumber* | **none** }]

undo cfd md *md-name*

Default

No MDs exist.

Views

System view

Predefined user roles

network-admin

Parameters

md *md-name*: Specifies the name of an MD, which is a string of 1 to 43 characters that can contain letters, numbers, and special characters such as grave accent (`), tilde (~), exclamation mark (!), at sign (@), number sign (#), dollar sign ($), percent (%), caret (^), ampersand (&), asterisk (*), brackets ({ }, ( ), [ ], < >), hyphen (-), underscore (_), plus (+), equal sign (=), vertical bar (|), colon (:), semicolon (;), quotation mark ('), comma (,), period (.), and slash (/).

index *index-value*: Specifies an MD index in the range of 1 to 4294967295. If you do not specify this option, the system automatically assigns the smallest index number that is not in use. As a best practice, use the index automatically assigned by the system.

level *level-value*: Specifies an MD level in the range of 0 to 7.

md-id: Specifies the MD name carried by packets sent by the MEP. If you do not provide this keyword, the MD name is represented by *md-name*.

dns *dns-name*: Specifies an MD name in the format of DNS name, where *dns-name* represents the DNS name.

mac *mac-address subnumber*: Specifies an MD name containing the MAC address and an integer. The *mac-address* argument represents the MAC address of the MD, and the *subnumber* argument is in the range of 0 to 65535.

none: Specifies that no MD name is carried in the packets sent by the MEP.

Usage guidelines

An MD name must be in compliant with the specifications in IEEE802.1ag-2007.

You can create only one MD with a specific level. MD cannot be created if you enter an invalid MD name or an existing MD name or the MD index is in use.

When deleting an MD, you will also delete the configurations related to that MD.

Examples

Create an MD named **test_md1**, with its level being 3.

```
<Sysname> system-view
[Sysname] cfd md test_md1 level 3
```

Create an MD named **test_md2**, and the MD name carried in the packet sent by the MEP comprises the MAC address 1-1-1 and integer 1.

```
<Sysname> system-view
[Sysname] cfd md test_md2 level 5 md-id mac 1-1-1 1
```

cfd mep

Use **cfd mep** to create a MEP.

Use **undo cfd mep** to delete a MEP.

Syntax

cfd mep *mep-id* **service-instance** *instance-id* { **inbound** | **outbound** }

undo cfd mep *mep-id* **service-instance** *instance-id*

Default

No MEPs exist.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

mep *mep-id*: Specifies the MEP ID, in the range of 1 to 8191.

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767.

inbound: Creates an inward-facing MEP.

outbound: Creates an outward-facing MEP.

Usage guidelines

In creating a MEP, the service instance you specified defines the MD and MA to which the MEP belongs.

You cannot create a MEP if the MEP ID is not included in the MEP list of the relevant service instance.

Follow these guidelines when you use the command:

- Configurations in Ethernet interface view take effect only on the current interface.
- Configurations in aggregate interface view take effect only on the current aggregate interface.
- If the MEP belongs to an MA that does not carry the VLAN attribute, configurations on a member port of an aggregation group take effect only on the current member port.
- If the MEP belongs to an MA that carries the VLAN attribute, configurations on a member port of an aggregation group take effect only when the member port leaves the aggregation group.

Examples

Configure a MEP list in service instance 5, and create inward-facing MEP 3 in service instance 5 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] cfd md test_md level 3
[Sysname] cfd service-instance 5 ma-id vlan-based md test_md vlan 100
[Sysname] cfd meplist 3 service-instance 5
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] cfd mep 3 service-instance 5 outbound
```

Related commands

cfd meplist

cfd meplist

Use **cfd meplist** to create a MEP list.

Use **undo cfd meplist** to delete a MEP list.

Syntax

cfd meplist *mep-list* **service-instance** *instance-id*

undo cfd meplist *mep-list* **service-instance** *instance-id*

Default

No MEP list is created.

Views

System view

Predefined user roles

network-admin

Parameters

meplist *mep-list*: Specifies a space-separated list of up to 10 MEP items. Each item specifies a MEP ID or a range of MEP IDs in the form of *mep-id 1* **to** *mep-id 2*. The value range for the MEP ID is 1 to 8191. The *mep-id 2* must be equal to or greater than *mep-id 1*.

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767.

Usage guidelines

A MEP list is a collection of local MEPs allowed to be configured and the remote MEPs to be monitored in the same MA.

Before creating a MEP list, create the relevant MD and service instance.

After you delete a MEP list, all local MEP configurations based on this list are deleted.

Examples

Create a MEP list that includes MEP 9 through MEP 15 in service instance 5.

```
<Sysname> system-view
[Sysname] cfd md test_md level 3
[Sysname] cfd service-instance 5 ma-id vlan-based md test_md vlan 100
[Sysname] cfd meplist 9 to 15 service-instance 5
```

Related commands

cfd md

cfd service-instance

cfd mip-rule

Use **cfd mip-rule** to configure the rules for generating MIPs.

Use **undo cfd mip-rule** to remove the rules for generating MIPs and the MIPs created in a service instance.

Syntax

cfd mip-rule { **default** | **explicit** } **service-instance** *instance-id*

undo cfd mip-rule [**default** | **explicit**] **service-instance** *instance-id*

Default

No rules for generating MIPs are configured and the system does not automatically generate any MIPs.

Views

System view

Predefined user roles

network-admin

Parameters

default: Specifies the default rule. If no lower-level MIP exists on an interface, a MIP is created on the current level. A MIP can be created even if no MEP is configured on the interface.

explicit: Specifies the explicit rule. If no lower-level MIP exists and a lower-level MEP exists on an interface, a MIP is created at the current level. A MIP can be created only when a lower-level MEP is created on the interface.

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767.

Usage guidelines

The system automatically generates MIPs on each port according to the rules configured.

Examples

Configure the MIP generation rule as default in service instance 5.

```
<Sysname> system-view
[Sysname] cfd mip-rule default service-instance 5
```

cfd service-instance

Use **cfd service-instance** to create a service instance.

Use **undo cfd service-instance** to remove a service instance.

Syntax

cfd service-instance *instance-id* **ma-id** { **icc-based** *ma-name* | **integer** *ma-num* | **string** *ma-name* | **vlan-based** [*vlan-id*] } [**ma-index** *index-value*] **md** *md-name* **vlan** *vlan-id*

undo cfd service-instance *instance-id*

Default

No service instances exist.

Views

System view

Predefined user roles

network-admin

Parameters

service-instance *instance-id*: Specifies the service instance ID in the range of 1 to 32767.

ma-id: Creates an MA.

icc-based *ma-name*: Specifies that an MA is identified by an ICC. The *ma-name* argument is a string of 1 to 13 characters.

integer *ma-num*: Specifies that an MA is identified by an integer, where the *ma-num* argument is in the range of 0 to 65535.

string *ma-name*: Specifies that an MA is identified by a string, where the *ma-name* argument is string of 1 to 45 characters that can contain letters, numbers, and special characters such as grave accent (`), tilde (~), exclamation mark (!), at sign (@), number sign (#), dollar sign ($), percent (%), caret (^), ampersand (&), asterisk (*), brackets ({ }, ( ), [ ], < >), hyphen (-), underscore (_), plus (+), equal sign (=), vertical bar (|), colon (:), semicolon (;), quotation mark ('), comma (,), period (.), and slash (/).

vlan-based [*vlan-id*]: Specifies that an MA is identified by a VLAN ID, where the *vlan-id* argument is in the range of 1 to 4094. If you do not provide the *vlan-id* argument, the VLAN ID specified by **vlan** *vlan-id* is used. If the **vlan** *vlan-id* option is not provided, you must specify the *vlan-id* argument for the **vlan-based** [*vlan-id*] option.

ma-index *index-value*: Specifies an MA index in the range of 1 to 4294967295. If you do not specify this option, the system automatically assigns the smallest index number that is not in use. As a best practice, use the index automatically assigned by the system.

md *md-name*: Specifies the name of an MD. The *md-name* argument is a string of 1 to 43 characters that can contain letters, numbers, and special characters such as grave accent (`), tilde (~), exclamation mark (!), at sign (@), number sign (#), dollar sign ($), percent (%), caret (^), ampersand (&), asterisk (*), brackets ({ }, ( ),[ ], < >), hyphen (-), underscore (_), plus (+), equal sign (=), vertical bar (|), colon (:), semicolon (;), quotation mark ('), comma (,), period (.), and slash (/).

vlan *vlan-id*: Specifies the VLAN that the MA serves. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

A service instance is indicated by an integer to represent an MA in an MD. An MA index uniquely identifies a specific MA in an MD. An MA index can be used in different MDs.

An MD name must be in compliant with the specifications in IEEE802.1ag-2007.

With the **vlan-based** [*vlan-id*] or **vlan** *vlan-id* option, the command creates an MA carrying the VLAN attribute. If you do not specify the option, the command creates an MA carrying no VLAN attribute.

You must create the relevant MD before creating a service instance with the MD name.

Deleting a service instance also deletes the configurations related to that service instance.

Deleting a service instance not only removes the connection between the service instance and the relevant MA, but also deletes the MA.

Examples

Create a level-3 MD named **test_md** and create service instance 5, in which the MA is identified by a VLAN and serves VLAN 100.

```
<Sysname> system-view
[Sysname] cfd md test_md level 3
[Sysname] cfd service-instance 5 ma-id vlan-based md test_md vlan 100
```

Related commands

cfd md

cfd slm

Use **cfd slm** to enable loss measurement (LM).

Syntax

cfd slm service-instance *instance-id* **mep** *mep-id* { **target-mac** *mac-address* | **target-mep** *target-mep-id* } [**dot1p** *dot1p-value*] [**number** *number*] [**interval** *interval*]

Views

Any view

Predefined user roles

network-admin

Parameters

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767.

mep *mep-id*: Specifies the source MEP by its ID in the range of 1 to 8191.

target-mac *mac-address*: Specifies the target MEP by its MAC address, which is in the format of H-H-H.

target-mep *target-mep-id*: Specifies the target MEP by its ID in the range of 1 to 8191.

dot1p *dot1p-value*: Specifies an 802.1p priority for LMM frames. The value range for the *dot1p-value* argument is 0 to 7. The default value is 7.

number *number*: Specifies the number of LMM frames to be sent. The value range for the *number* argument is 2 to 10, and the default is 5.

interval *interval*: Specifies the LMM frame sending interval, in seconds. The value takes 1 or 10. The default value is 1.

Usage guidelines

The LM function measures the frame loss between the source and target MEPs by using LMM frames and LMR frames.

Examples

Enable the LM function to measure the frame loss between source MEP 1101 and target MEP 2001 in service instance 1.

```
<Sysname> cfd slm service-instance 1 mep 1101 target-mep 2001
Reply from 0010-fc00-6512
Far-end frame loss: 10    Near-end frame loss: 20
Reply from 0010-fc00-6512
Far-end frame loss: 40    Near-end frame loss: 40
Reply from 0010-fc00-6512
Far-end frame loss: 0     Near-end frame loss: 10
Reply from 0010-fc00-6512
Far-end frame loss: 30    Near-end frame loss: 30

Average
Far-end frame loss: 20    Near-end frame loss: 25
Far-end frame loss rate: 25.00%      Near-end frame loss rate: 32.00%
Sent LMMs: 5    Received: 5    Lost: 0
```

Table 5 Command output

Field	Description
Reply from 0010-fc00-6512	LMR frames returned from the target MEP with MAC address 0010-FC00-6512.
Far-end frame loss	Number of lost frames on the target MEP.
Near-end frame loss	Number of lost frames on the source MEP.
Far-end frame loss rate	Frame loss ratio on the target MEP.
Near-end frame loss rate	Frame loss ratio on the source MEP.
Average	Average number of lost frames.
Sent LMMs	Number of sent LMM frames.
Received	Number of received LMR frames.
Lost	Number of lost LMR frames.

cfd tst

Use **cfd tst** to enable test (TST).

Syntax

cfd tst service-instance *instance-id* **mep** *mep-id* { **target-mac** *mac-address* | **target-mep** *target-mep-id* } [**number** *number*] [**length-of-test** *length*] [**pattern-of-test** { **all-zero** | **prbs** } [**with-crc**]]

Views

Any view

Predefined user roles

network-admin

Parameters

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767.

mep *mep-id*: Specifies the source MEP by its ID in the range of 1 to 8191.

target-mac *mac-address*: Specifies the target MEP by its MAC address, which is in the format of H-H-H.

target-mep *target-mep-id*: Specifies the target MEP by its ID in the range of 1 to 8191.

number *number*: Specifies the number of sent TST frames. The value range for the *number* argument is 1 to 10, and the default is 5.

length-of-test *length*: Specifies the length of the Test TLV (Type/Length/Value) in the TST frame. The value range for the *length* argument is 4 to 1400, in bytes. The default value is 64.

pattern-of-test { **all-zero** | **prbs** } [**with-crc**]: Specifies the pattern of the Test TLV in the TST frame:

- **all-zero** (all-zero value without CRC-32), which is the default pattern.
- **prbs** (pseudo random bit sequence without CRC-32).
- **all-zero with-crc** (all-zero value with CRC-32).
- **prbs with-crc** (pseudo random bit sequence with CRC-32).

Usage guidelines

The TST function detects bit errors between the source and target MEPs by using TST frames.

To view the TST test result, use the **display cfd tst** command on the target MEP.

Examples

Enable the TST function to test the bit errors between source MEP 1101 and target MEP 1003 in service instance 1.

```
<Sysname> cfd tst service-instance 1 mep 1101 target-mep 1003
5 TSTs have been sent. Please check the result on the remote device.
```

Related commands

display cfd tst

reset cfd tst

display cfd ais

Use **display cfd ais** to display the AIS configuration and information on the specified MEP or all MEPs.

Syntax

display cfd ais [**service-instance** *instance-id* [**mep** *mep-id*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767. If you do not specify this option, the command displays the AIS configuration and information for all service instances.

mep *mep-id*: Specifies a MEP by its ID in the range of 1 to 8191. If you do not specify this option, the command displays the AIS configuration and information for all MEPs.

Examples

Display the AIS configuration and information for all the MEPs in all service instances.

```
<Sysname> display cfd ais
Service instance: 5
AIS level: 4    AIS period: 1s
MEP ID: 1
AIS condition: yes   Time to enter the condition: 2013/01/22 10:43:57
AIS state machine: Previous state: NO_RECEIVE
                   Current state: RECEIVE
MEP ID: 2
AIS condition: yes   Time to enter the condition: 2013/01/22 10:43:57
AIS state machine: Previous state: NO_RECEIVE
                   Current state: RECEIVE

Service instance: 20
AIS level: 3    AIS period: 60s
MEP ID: 10
AIS condition: yes   Time to enter the condition: 2013/01/22 10:43:57
AIS state machine: Previous state: NO_RECEIVE
                   Current state: RECEIVE

Service instance: 100
AIS level: 6    AIS period: 1s
MEP ID: 20
AIS condition: no    Time to enter the condition: 2013/01/22 11:40:01
AIS state machine: Previous state: IDLE
                   Current state: NO_RECEIVE

MEP ID: 50
AIS condition: no    Time to enter the condition: -
AIS state machine: Previous state: IDLE
                   Current state: NO_RECEIVE
```

Table 6 Command output

Field	Description
Service instance	Service instance of the MEP.
AIS level	AIS frame transmission level.
AIS period	AIS frame transmission period.
AIS condition	AIS status: • **yes**—AIS is running. • **no**—AIS is not running.
Time to enter the condition	Time when the AIS status began. (**-** means AIS is enabled but the MEP does not receive any AIS frame.)
AIS state machine	AIS frame receiving state machine.
Previous state	Previous state: • **IDLE**—Not activated. • **NO_RECEIVE**—Activated. • **RECEIVE**—AIS frames are received.
Current state	Current state: • **IDLE**—Not activated. • **NO_RECEIVE**—Activated. • **RECEIVE**—AIS frames are received.

display cfd ais-track link-status

Use **display cfd ais-track link-status** to display the configuration and information of the AIS associated with the port status.

Syntax

display cfd ais-track link-status [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify this option, the command displays the configuration and information of the AIS associated with the status of all ports.

Examples

Display the configuration and information of the AIS associated with the status of all ports.

```
<Sysname> display cfd ais-track link-status
AIS tracking link-status is enabled.

Interface GigabitEthernet1/0/1:
AIS level: 5          AIS period: 1s
```

```
Configured VLANs: 1, 10-100, 103
Send VLANs: 1, 10-100, 103
AIS condition: yes     Time to enter the condition: 2013/02/26 10:43:57

Interface GigabitEthernet1/0/2:
AIS level: 5          AIS period: 1s
Configured VLANs: 1-4094
Send VLANs: 1-2000
AIS condition: yes     Time to enter the condition: 2013/02/26 10:44:57
```

Table 7 Command output

Field	Description
AIS tracking link-status is enabled	Port status-AIS collaboration is enabled.
AIS tracking link-status is disabled	Port status-AIS collaboration is disabled.
Interface	Port that collaborates with AIS.
AIS level	EAIS frame transmission level on the port.
AIS period	EAIS frame transmission period on the port.
Configured VLANs	VLANs where the EAIS frames can be transmitted.
Send VLANs	Actual VLANs where the EAIS frames can be transmitted.
AIS condition	EAIS frame sending status: • **yes**—EAIS frames are being sent. • **no**—No EAIS frame is being sent.
Time to enter the condition	Time when the EAIS frame sending started.

display cfd dm one-way history

Use **display cfd dm one-way history** to display the one-way DM result.

Syntax

display cfd dm one-way history [**service-instance** *instance-id* [**mep** *mep-id*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767. If you do not specify this option, the command displays the one-way DM results for all service instances.

mep *mep-id*: Specifies a MEP by its ID in the range of 1 to 8191. If you do not specify this option, the command displays the one-way DM results for all MEPs.

Usage guidelines

The one-way DM results for all inward-facing MEPs in a service instance are the same.

Examples

Display the one-way DM results for all the MEPs in all service instances.

```
<Sysname> display cfd dm one-way history
Service instance: 1
MEP ID: 1003
Sent 1DM total number: 0
Received 1DM total number: 5
Frame delay: 10ms 9ms 11ms 5ms 5ms
Delay average: 8ms
Frame delay variation: 5ms 4ms 6ms 0ms 0ms
Variation average: 3ms
MEP ID: 1004
Sent 1DM total number: 0
Received 1DM total number: 5
Frame delay: 10ms 9ms 11ms 5ms 5ms
Delay average: 8ms
Delay variation: 5ms 4ms 6ms 0ms 0ms
Variation average: 3ms

Service instance: 2
No MEP exists in the service instance.

Service instance: 3
MEP ID: 1023
Sent 1DM total number: 5
Received 1DM total number: 10
Frame delay: 20ms 9ms 8ms 7ms 1ms 5ms 13ms 17ms 9ms 10ms
Delay average: 9ms
Delay variation: 19ms 8ms 7ms 6ms 0ms 4ms 12ms 16ms 8ms 9ms
Variation average: 8ms

Service instance: 4
MEP ID: 1023
Sent 1DM total number: 77
Received 1DM total number: 0
```

Table 8 Command output

Field	Description
Service instance	Service instance of the MEP.
Sent 1DM total number	Number of sent 1DM frames.
Received 1DM total number	Number of received 1DM frames.
Delay average	Average frame delay.
Delay variation	Frame delay variation.
Variation average	Average frame delay variation.

Related commands

cfd dm one-way

reset cfd dm one-way history

display cfd linktrace-reply

Use **display cfd linktrace-reply** to display information about the LTRs received by a MEP.

Syntax

display cfd linktrace-reply [**service-instance** *instance-id* [**mep** *mep-id*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767. If you do not specify this option, the command displays the LTR information for all service instances.

mep *mep-id*: Specifies the ID of a MEP, in the range of 1 to 8191. If you do not specify this option, the command displays the LTR information for all MEPs.

Usage guidelines

This command displays only information about LTRs received by execution of the **cfd linktrace** command.

Examples

Display the LTR information saved on all the MEPs in every service instance.

```
[Sysname] display cfd linktrace-reply
Service instance: 1       MEP ID: 1003
MAC address               TTL     Last MAC          Relay action
0000-fc00-6505            63      0000-fc00-6504    MPDB
000f-e269-a852            62      0000-fc00-6505    FDB
0000-fc00-6508            61      000f-e269-a852    Hit
Service instance: 2       MEP ID: 1023
MAC address               TTL     Last MAC          Relay action
0000-fc00-6508            61      000f-e269-a852    Hit
```

Table 9 Command output

Field	Description
Service instance	Service instance to which the MEPs that send LTMs belong.
MEP ID	ID of the MEP that sends LTMs.
MAC address	Source MAC address in the LTR.
TTL	TTL of the LTM when it passes the device.
Last MAC	MAC address of the last-hop device the LTM passes.

Field	Description
Relay action	Indicates whether the forwarding device found the destination MAC address in its MAC address table. When the standard version (IEEE 802.1ag) of CFD is used: • **Hit**—The current device is the destination device. • **FDB**—The forwarding device found the destination MAC address. • **MPDB**—The destination MAC address is not found, or the destination MAC address is found in the MEP or MIP database.

Related commands

cfd linktrace

display cfd linktrace-reply auto-detection

Use **display cfd linktrace-reply auto-detection** to display information about the LTRs received as responses to the automatically sent LTMs.

Syntax

display cfd linktrace-reply auto-detection [**size** *size-value*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

size *size-value*: Specifies the times of recent auto-detections, in the range of 1 to 100. If you do not specify this option, the command displays all information in the buffer.

Usage guidelines

This command displays only information about LTRs received by execution of the **cfd linktrace auto-detection** command.

Examples

Display the contents of the LTRs received as responses to the LTMs automatically sent.

```
<Sysname> display cfd linktrace-reply auto-detection
Service instance: 1       MEP ID: 1003    Time: 2013/05/22 10:43:57
Target MEP ID: 2005       TTL: 64
MAC address               TTL     Last MAC          Relay action
0000-fc00-6505            63      0000-fc00-6504    MPDB
000f-e269-a852            62      0000-fc00-6505    FDB
0000-fc00-6508            61      000f-e269-a852    Hit
Service instance: 2       MEP ID: 1023    Time: 2013/05/22 10:44:06
Target MEP ID: 2025       TTL: 64
MAC address               TTL     Last MAC          Relay action
0000-fc00-6508            61      000f-e269-a852    Hit
```

Table 10 Command output

Field	Description
Service instance	Service instance to which the MEPs that sent LTMs belong.
MEP ID	ID of the MEP that sends LTMs.
Time	Time of the LTMs automatically sent.
Target MEP ID	ID of the target MEP.
TTL	Initial TTL of the automatically sent LTMs.
MAC address	Source MAC address in the LTRs.
TTL	TTL of the LTM when it passes the device.
Last MAC	MAC address of the last-hop device the LTM passes.
Relay action	Indicates whether the forwarding device found the destination MAC address in its MAC address table. When the standard version (IEEE 802.1ag) of CFD is used: • **Hit**—The current device is the destination device. • **FDB**—The forwarding device found the destination MAC address. • **MPDB**—The destination MAC address is not found, or the destination MAC address is found in the MEP or MIP database.

Related commands

`cfd linktrace auto-detection`

display cfd md

Use **`display cfd md`** to display the MD configuration information.

Syntax

`display cfd md`

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the MD configuration information.

```
<Sysname> display cfd md
CFD is enabled.
Maintenance domains configured: 4 in total
Level  Index      Maintenance domain                          MD format  MD ID
0      1          md_0                                        CHARSTRING md_0
1      2          md_1                                        DNS        dns1
2      3          md_2                                        MAC        0001-00
01-0001-1
3      4          md_3                                        NONE       Without
 ID
```

Table 11 Command output

Field	Description
Maintenance domains configured	Number of MDs configured.
Level	Level of MD.
Index	MD index.
Maintenance domain	Name of MD.
MD format	MD name format: • **CHARSTRING**—Character string. • **DNS**—DNS name. • **MAC**—MAC address and an integer. • **NONE**—No MD name is carried.
MD ID	MD ID value: • A character string if the MD format is **CHARSTRING**. • A DNS name if the MD format is **DNS**. • A MAC address-subnumber if the MD format is **MAC**. • No ID if the MD format is **NONE**.

display cfd mep

Use **display cfd mep** to display the attribute and operating information for a MEP.

Syntax

display cfd mep *mep-id* **service-instance** *instance-id*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

mep *mep-id*: Specifies a MEP by its ID in the range of 1 to 8191.

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767.

Examples

Display the attribute and operating information for MEP 50 in service instance 1.

```
<Sysname> display cfd mep 50 service-instance 1
Interface: GigabitEthernet1/0/2
Maintenance domain: md_0
Maintenance domain index: 1
Maintenance association: ma_0
Maintenance association index: 1
Level: 0        VLAN: 1         Direction: Outbound
Current state: Active          CCM send: Enabled
FNG state: FNG_DEFECT_REPORTED
```

```
CCM:
Current state: CCI_WAITING
Interval: 1s        SendCCM: 12018

Loopback:
NextSeqNumber: 8877
SendLBR: 0          ReceiveInOrderLBR: 0          ReceiveOutOrderLBR: 0

Linktrace:
NextSeqNumber: 8877
SendLTR: 0          ReceiveLTM: 0

No CCM received from some remote MEPs.

One or more streams of error CCMs is received. The last received CCM:
Maintenance domain: (Without ID)
Maintenance association: matest1
MEP ID: 5      Sequence Number:0x50A
MAC Address: 0011-2233-4402
Received Time: 2013/03/06 13:01:34

One or more streams of cross-connect CCMs is received. The last received CCM:
Maintenance domain: mdtest1
Maintenance association:matest1
MEP ID: 6      Sequence Number:0x63A
MAC Address: 0011-2233-4401
Received Time: 2013/03/06 13:01:34

Some other MEPs are transmitting the RDI bit.
```

Table 12 Command output

Field	Description
Interface	Interface on which the MEP is configured.
Maintenance domain	MD to which the MEP belongs. (If the MD does not have a name, this field is displayed as **Without ID**.)
Maintenance domain index	Index of the MD to which the MEP belongs..
Maintenance association	MA to which the MEP belongs.
Maintenance association index	Index of the MA to which the MEP belongs.
Level	Level of the MD.
VLAN	VLAN to which the MA belongs.
Direction	Direction of the MEPs.
Current state	State of MEP: • **Active**. • **Inactive**.
CCM send	Whether the MEP sends CCM.

Field	Description
FNG state	State of FNG (Fault Notification Generator): • **FNG_RESET**—A fault has been cleared. • **FNG_DEFECT**—A fault has been detected. • **FNG_REPORT_DEFECT**—Report a fault. • **FNG_DEFECT_REPORTED**—A fault has been reported. • **FNG_DEFECT_CLEARING**—A fault is being cleared. If this field is not supported, a hyphen (-) is displayed.
CCM	Information related to CCM.
Current state	State of CCMs sent: • **CCI_IDLE**—Initial state. • **CCI_WAITING**—Sending state. If this field is not supported, a hyphen (-) is displayed.
Interval	Interval to send CCM. **Not supported** means the MEP does not support CCM sending.
SendCCM	Number of CCMs that have been sent by the MEPs. If this field is not supported, a hyphen (-) is displayed.
Loopback	Information related to Loopback.
NextSeqNumber	Sequence number of the next LBM to be sent.
SendLBR	Number of LBRs that have been sent. If the MEP is inward-facing, the number of LBRs will not be counted.
ReceiveInOrderLBR	Number of LBRs received in correct sequence.
ReceiveOutOrderLBR	Number of LBRs received out of order.
Linktrace	Information related to linktrace.
NextSeqNumber	Sequence number of the next LTM to be sent.
SendLTR	Number of LTRs sent. If the MEP is inward-facing, the number of LTRs will not be counted.
ReceiveLTM	Number of LTMs received.
No CCM received from some remote MEPs.	Failure to receive CCMs from some remote MEPs. (This information is displayed only when some CCMs are lost.)
One or more streams of error CCMs is received. The last received CCM:	Display the content of the last error CCM when one or more error CCMs are received. (This information is displayed only when error CCMs are received.)
Maintenance domain	MD of the last error CCM. If this field is not supported, a hyphen (-) is displayed.
Maintenance association	MA of the last error CCM. If this field is not supported, a hyphen (-) is displayed.
MEP	ID of the MEP that sent the last error CCM. If this field is not supported, a hyphen (-) is displayed.
Sequence Number	Sequence number of the last error CCM. If this field is not supported, a hyphen (-) is displayed.
Received Time	Time when the last error CCM is received. If this field is not supported, a hyphen (-) is displayed.

Field	Description
One or more streams of cross-connect CCMs is received. The last received CCM:	Cross-connect CCMs are received, and the content of the last cross-connect CCM is displayed. (This information is displayed only when cross-connect CCMs are received.)
Some other MEPs are transmitting the RDI bit.	CCMs with the RDI flag bits set are received from other MEPs. (This information is displayed only when this type of CCMs are received.)

display cfd meplist

Use **display cfd meplist** to display the MEP list in a service instance.

Syntax

display cfd meplist [**service-instance** *instance-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767. If you do not specify this option, the command displays MEP lists in all service instances.

Examples

Display the MEP list in service instance 5.

```
<Sysname> display cfd meplist service-instance 5
Service instance: 5
MEP list: 1 to 20, 30, 50.
```

display cfd mp

Use **display cfd mp** to display the MP information.

Syntax

display cfd mp [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify this option, the command displays MP information for all ports.

Usage guidelines

The output is arranged by port name. On a port, the output shows MPs that serve VLANs, and then shows MPs that do not serve any VLANs. The MPs that serve VLANs are displayed in the ascending VLAN ID order. Within the same VLAN, the output is in the order of MIPs and MEPs (from high to low level). The MEPs that do not serve any VLANs are displayed by level (from high to low).

Examples

Display the MP information on all ports.

```
<Sysname> display cfd mp
Interface GigabitEthernet1/0/1   VLAN 100
MIP              Level: 2    Service instance: 102
Maintenance domain: md_2
Maintenance domain index: 3
Maintenance association: ma_2
Maintenance association index: 3

MEP ID: 101      Level: 1    Service instance: 101    Direction: Inbound
Maintenance domain: md_1
Maintenance domain index: 2
Maintenance association: ma_1
Maintenance association index: 2

MEP ID: 100      Level: 0    Service instance: 100    Direction: Outbound
Maintenance domain: md_0
Maintenance domain index: 1
Maintenance association: ma_0
Maintenance association index: 1
```

Table 13 Command output

Field	Description
Interface GigabitEthernet1/0/1 VLAN 100	MP configuration of VLAN 100 on GigabitEthernet 1/0/1.
MIP	A MIP in the MP.
Level	MD level to which the MP belongs.
Service instance	Service instance to which the MP belongs.
Maintenance domain	MD to which the MP belongs.
Maintenance domain index	Index of the MD to which the MP belongs.
Maintenance association	MA to which the MP belongs.
Maintenance association index	Index of the MA to which the MP belongs.
Direction	Direction of the MEP, inbound or outbound.

display cfd remote-mep

Use **display cfd remote-mep** to display information about a remote MEP.

Syntax

display cfd remote-mep service-instance *instance-id* **mep** *mep-id*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767.

mep *mep-id*: Specifies a MEP by its ID in the range of 1 to 8191.

Examples

Display remote MEP information for MEP 10 in service instance 4.

```
<Sysname> display cfd remote-mep service-instance 4 mep 10
MEP ID   MAC address      State        Time                 MAC status
20       00e0-fc00-6565   OK           2013/03/06 02:36:38  UP
30       00e0-fc27-6502   OK           2013/03/06 02:36:38  DOWN
40       00e0-fc00-6510   FAILED       2013/03/06 02:36:39  DOWN
50       00e0-fc52-baa0   OK           2013/03/06 02:36:44  DOWN
60       0010-fc00-6502   OK           2013/03/06 02:36:42  DOWN
```

Table 14 Command output

Field	Description
MEP ID	ID of the remote MED.
MAC address	MAC address of the remote MEP device. If this field is not supported, a hyphen (-) is displayed.
State	Running state of the remote MEP: • **OK**. • **FAILED**.
Time	Time when the remote MEP entered the **FAILED** or **OK** state for the last time. If this field is not supported, a hyphen (-) is displayed.
MAC status	State of the interface indicated by the last CCM received from the remote MEP: • **UP**—The interface is ready to pass packets. • **DOWN**—The interface cannot pass packets. • **TESTING**—The interface is in some test mode. • **UNKNOWN**—The interface status cannot be determined. • **DORMANT**—The interface is not in a state to pass packets. Instead, it is in a pending state, waiting for some external event. • **NOT-PRESENT**—Some component of the interface is missing. • **LLD**—The interface is down due to state of the lower layer interfaces. If this field is not supported, a hyphen (-) is displayed.

display cfd service-instance

Use **display cfd service-instance** to display the configuration information of service instances.

Syntax

display cfd service-instance [*instance-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

instance-id: Specifies a service instance ID in the range of 1 to 32767. If you do not specify this argument, the command displays configuration information for all service instances.

Examples

Display the configuration information of all service instances.

```
<Sysname> display cfd service-instance
Service instances configured (2 in total):
Service instance 5:
Maintenance domain: md_5
Maintenance domain index: 5
Maintenance association: ma_5
Maintenance association index: 5
Level: 5  VLAN: 5   MIP rule: NONE   CCM interval: 1s   Direction: Inbound
MEP ID: 730  Interface: GigabitEthernet1/0/1

Service instance 6:
Maintenance domain: (Without ID)
Maintenance domain index: 6
Maintenance association: ma_6
Maintenance association index: 6
Level: 6  VLAN: 6   MIP rule: NONE   CCM interval: 1s   Direction: Outbound
MEP ID: 731  Interface: GigabitEthernet1/0/2
```

Table 15 Command output

Field	Description
Service instances are configured.	Number of service instances configured.
Service instance	Service instance ID.
Maintenance domain	MD of the service instance. (If the MD does not have a name, this field displays **Without ID**.)
Maintenance domain index	Index of the MD to which the service instance belongs.
Maintenance association:	MA of the service instance.
Maintenance association index	Index of the MA to which the service instance belongs.
Level	MD level.
VLAN	VLAN to which the MA belongs.
MIP rule	MIP generation rules configured on the service instance.
CCM interval	Interval to send CCMs.

Field	Description
Direction	Direction of the MEPs configured on the service instance.
MEP ID	ID of MEPs configured on the service instance.
Interface	Interface of the MEP configured on the service instance.

display cfd status

Use **display cfd status** to display the CFD and AIS status.

Syntax

display cfd status

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the CFD and AIS status.

```
<Sysname> display cfd status
CFD is enabled.
AIS is disabled.
```

display cfd tst

Use **display cfd tst** to display the TST result.

Syntax

display cfd tst [**service-instance** *instance-id* [**mep** *mep-id*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767. If you do not specify this option, the command displays the TST results for all service instances.

mep *mep-id*: Specifies a MEP by its ID in the range of 1 to 8191. If you do not specify this option, the command displays the TST results for all MEPs.

Usage guidelines

The TST DM results for all inward-facing MEPs in a service instance are the same.

Examples

Display the TST results for all the MEPs in all service instances.

```
<Sysname> display cfd tst
Service instance: 1
MEP ID: 1003
Sent TST total number: 0
Received TST total number: 5
Received from 0010-fc00-6510, Bit True,  sequence number 0
Received from 0010-fc00-6510, Bit True,  sequence number 1
Received from 0010-fc00-6510, Bit True,  sequence number 2
Received from 0010-fc00-6510, Bit True,  sequence number 3
Received from 0010-fc00-6510, Bit True,  sequence number 4
MEP ID: 1004
Sent TST total number: 5
Received TST total number: 0

Service instance: 2
No MEP exists in the service instance.

Service instance: 3
MEP ID: 1023
Sent TST total number: 5
Received TST total number: 0
```

Table 16 Command output

Field	Description
Service instance	Service instance of the MEP.
Sent TST total number	Number of sent TST frames.
Received TST total number	Number of received TST frames.
Received from 0010-fc00-6510, Bit True, sequence number 0	TST frame with sequence number 0 was received from the MEP with MAC address 0010-FC00-6510: • **Bit True**—No bit error occurred. • **Bit False**—Bit errors occurred.

Related commands

cfd tst

reset cfd tst

reset cfd dm one-way history

Use **reset cfd dm one-way history** to clear the one-way DM result.

Syntax

reset cfd dm one-way history [**service-instance** *instance-id* [**mep** *mep-id*]]

Views

User view

Predefined user roles

network-admin

Parameters

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767. If you do not specify this option, the command clears the one-way DM results for all service instances.

mep *mep-id*: Specifies a MEP by its ID in the range of 1 to 8191. If you do not specify this option, the command clears the one-way DM results for all MEPs.

Usage guidelines

Clearing the one-way DM result for an inward-facing MEP clears all one-way DM results for the service instance where the inward-facing MEP resides.

Examples

Clear the one-way DM results for all MEPs in all service instances.

```
<Sysname> reset cfd dm one-way history
```

Related commands

cfd dm one-way

display cfd dm one-way history

reset cfd tst

Use **reset cfd tst** to clear the TST result.

Syntax

reset cfd tst [**service-instance** *instance-id* [**mep** *mep-id*]]

Views

User view

Predefined user roles

network-admin

Parameters

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767. If you do not specify this option, the command clears the TST results for all service instances.

mep *mep-id*: Specifies a MEP by its ID in the range of 1 to 8191. If you do not specify this option, the command clears the TST results for all MEPs.

Usage guidelines

Clearing the TST result for an inward-facing MEP clears all TST results for the service instance where the inward-facing MEP resides.

Examples

Clear the TST results for all MEPs in all service instances.

```
<Sysname> reset cfd tst
```

Related commands

cfd tst

display cfd tst

Contents

DLDP commands

display dldp

Use **display dldp** to display DLDP configuration.

Syntax

display dldp [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify this option, the command displays global and port-specific DLDP configuration.

Examples

Display global and port-specific DLDP configuration.

```
<Sysname> display dldp
 DLDP global status: Enabled
 DLDP advertisement interval: 5s
 DLDP authentication-mode: Simple
 DLDP authentication-password: ******
 DLDP unidirectional-shutdown mode: Auto
 DLDP delaydown-timer value: 1s
 Number of enabled ports: 2

Interface GigabitEthernet1/0/1
 DLDP port state: Bidirectional
 DLDP port unidirectional-shutdown mode: None
 DLDP initial-unidirectional-delay: 100s
 Number of the port’s neighbors: 1
  Neighbor MAC address: 0023-8956-3600
  Neighbor port index: 79
  Neighbor state: Confirmed
  Neighbor aged time: 13s
  Neighbor echo time: -

Interface GigabitEthernet1/0/2
 DLDP port state: Inactive
 DLDP port unidirectional-shutdown mode: None
 DLDP initial-unidirectional-delay: 100s
 Number of the port’s neighbors: 0 (Maximum number ever detected: 1)
```

Display the DLDP configuration of GigabitEthernet 1/0/1.

```
<Sysname> display dldp interface gigabitethernet 1/0/1
Interface GigabitEthernet1/0/1
 DLDP port state: Bidirectional
 DLDP port unidirectional-shutdown mode: None
 DLDP initial-unidirectional-delay: 100s
 Number of the port’s neighbors: 1
  Neighbor MAC address: 0023-8956-3600
  Neighbor port index: 79
  Neighbor state: Confirmed
  Neighbor aged time: 13s
  Neighbor echo time: -
```

Table 1 Command output

Field	Description
DLDP global status	Global DLDP state (Enabled or Disabled).
DLDP advertisement interval	Interval for sending Advertisement packets (in seconds) to maintain neighbor relations.
DLDP authentication-mode	DLDP authentication mode (None, Simple, or MD5).
DLDP authentication-password	Password for DLDP authentication: • **********—The password has been configured. • **Not configured**—The authentication mode has been configured but no password is configured.
DLDP unidirectional-shutdown mode	Global port shutdown mode (auto, manual, or hybrid) after unidirectional links are detected.
DLDP port unidirectional-shutdown mode	Port shutdown mode for the interface (auto, manual, or hybrid) after unidirectional links are detected. If no port shutdown mode is configured for an interface, this field displays **None**.
DLDP delaydown-timer value	Setting of the DelayDown timer, in seconds.
Number of enabled ports	Number of the DLDP-enabled ports.
Interface	Index of a DLDP-enabled port.
DLDP port state	DLDP state on a port: • **Bidirectional**. • **Inactive**. • **Initial**. • **Unidirectional**.
DLDP initial-unidirectional-delay	Delay time in seconds for DLDP to block the interface upon an Initial-to-Unidirectional state transition.
Number of the port’s neighbors	Current number of neighbors.
Maximum number ever detected	Maximum number of neighbors once detected on the port. This field appears only when the current number of neighbors is different from the maximum number of neighbors once detected.
Neighbor MAC address	Bridge MAC address of the device where the neighbor resides.
Neighbor port index	Neighbor port index.
Neighbor state	Neighbor state (Confirmed or Unconfirmed).
Neighbor aged time	Neighbor aging time.

Field	Description
Neighbor echo time	Number of seconds remaining before the Echo timer expires. The Echo timer starts when the Entry timer expires. The neighbor information is deleted when the Echo timer expires. A hyphen (-) indicates that the Echo timer has not started.

display dldp statistics

Use **display dldp statistics** to display DLDP packet statistics.

Syntax

display dldp statistics [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify this option, the command displays DLDP packet statistics for all interfaces.

Examples

Display DLDP packet statistics for all interfaces.

```
<Sysname> display dldp statistics
Interface GigabitEthernet1/0/1
 Packets sent: 6
 Packets received: 5
 Invalid packets received: 2
 Loopback packets received: 0
 Authentication-failed packets received: 0
 Valid packets received: 3

Interface GigabitEthernet1/0/2
 Packets sent: 7
 Packets received: 7
 Invalid packets received: 3
 Loopback packets received: 0
 Authentication-failed packets received: 0
 Valid packets received: 4
```

Table 2 Command output

Field	Description
Interface	Port index.
Packets sent	Total number of DLDP packets sent.

Field	Description
Packets received	Total number of DLDP packets received.
Invalid packets received	Number of the invalid packets received.
Loop packets received	Number of the loopback packets received.
Authentication failed packets received	Number of the received packets that failed to pass the authentication.
Valid packets received	Number of the valid packets received.

Related commands

`reset dldp statistics`

dldp authentication-mode

Use **`dldp authentication-mode`** to configure DLDP authentication.

Use **`undo dldp authentication-mode`** to restore the default.

Syntax

`dldp authentication-mode` { **`md5`** | **`none`** | **`simple`** }

`undo dldp authentication-mode`

Default

DLDP authentication mode is **none**.

Views

System view

Predefined user roles

network-admin

Parameters

`md5`: Specifies the MD5 authentication mode.

none: Specifies not to perform authentication.

`simple`: Specifies the plaintext authentication mode.

Usage guidelines

To enable DLDP to operate correctly, make sure the DLDP authentication modes and the passwords configured on the two ends of a link are the same.

If you do not configure the authentication password after you configure the authentication mode, the authentication mode is **none** no matter which authentication mode you configure.

Examples

Configure to perform plaintext authentication and set the password to **abc** (assuming that Device A and Device B are connected by a DLDP link).

- Configure Device A:

```
<DeviceA> system-view
[DeviceA] dldp authentication-mode simple
[DeviceA] dldp authentication-password simple abc
```

- Configure Device B:

```
<DeviceB> system-view
[DeviceB] dldp authentication-mode simple
[DeviceB] dldp authentication-password simple abc
```

Related commands

display dldp

dldp authentication-password

dldp authentication-password

Use **dldp authentication-password** to configure the password for DLDP authentication.

Use **undo dldp authentication-password** to restore the default.

Syntax

dldp authentication-password { **cipher** | **simple** } *string*

undo dldp authentication-password

Default

No DLDP authentication password is configured.

Views

System view

Predefined user roles

network-admin

Parameters

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 16 characters. Its encrypted form is a case-sensitive string of 1 to 53 characters.

Usage guidelines

To enable DLDP to operate correctly, make sure the DLDP authentication modes and the passwords configured on the two ends of a link are the same.

If you do not configure the authentication password after you configure the authentication mode, the authentication mode is **none** no matter which authentication mode you configure.

Examples

Configure to perform plaintext authentication and set the password to **abc** (assuming that Device A and Device B are connected by a DLDP link).

- Configure Device A:

```
<DeviceA> system-view
[DeviceA] dldp authentication-mode simple
[DeviceA] dldp authentication-password simple abc
```

- Configure Device B:

```
<DeviceB> system-view
[DeviceB] dldp authentication-mode simple
[DeviceB] dldp authentication-password simple abc
```

Related commands

display dldp

dldp authentication-mode

dldp delaydown-timer

Use **dldp delaydown-timer** to set the DelayDown timer.

Use **undo dldp delaydown-timer** to restore the default.

Syntax

dldp delaydown-timer *time*

undo dldp delaydown-timer

Default

The setting of the DelayDown timer is 1 second.

Views

System view

Predefined user roles

network-admin

Parameters

time: Specifies the DelayDown timer in the range of 1 to 5 seconds.

Usage guidelines

The DelayDown timer configured by using this command applies to all DLDP-enabled ports.

Examples

Set the DelayDown timer to 2 seconds.

```
<Sysname> system-view
[Sysname] dldp delaydown-timer 2
```

Related commands

display dldp

dldp enable

Use **dldp enable** to enable DLDP on a port.

Use **undo dldp enable** to restore the default.

Syntax

dldp enable [**initial-unidirectional-delay** *time*]

undo dldp enable

Default

DLDP is disabled on a port, and when DLDP is enabled, a port is blocked immediately upon an Initial-to-Unidirectional state transition.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

initial-unidirectional-delay *time*: Specifies the delay time for DLDP to block a port upon an Initial-to-Unidirectional state transition. The value range for the *time* argument is 60 to 300 seconds. If you do not specify this option, DLDP blocks the port immediately upon an Initial-to-Unidirectional state transition.

Usage guidelines

DLDP can take effect only after you enable it globally and on a port.

When enabling DLDP on a port, you can set the delay time for DLDP to block the port upon an Initial-to-Unidirectional state transition. If the port does not enter Bidirectional state when the delay time expires, DLDP blocks the port.

Examples

Enable DLDP globally, and enable DLDP on GigabitEthernet 1/0/1 and set a delay time of 100 seconds for DLDP to block the port upon an Initial-to-Unidirectional state transition.

```
<Sysname> system-view
[Sysname] dldp global enable
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dldp enable initial-unidirectional-delay 100
```

Related commands

display dldp

dldp global enable

dldp global enable

Use **dldp global enable** to enable DLDP globally.

Use **undo dldp global enable** to disable DLDP globally.

Syntax

dldp global enable

undo dldp global enable

Default

DLDP is disabled globally.

Views

System view

Predefined user roles

network-admin

Usage guidelines

DLDP can take effect only after you enable it globally and on a port.

Examples

Enable DLDP globally.

```
<Sysname> system-view
[Sysname] dldp global enable
```

Related commands

display dldp

dldp enable

dldp interval

Use **dldp interval** to set the interval for sending Advertisement packets.

Use **undo dldp interval** to restore the default.

Syntax

dldp interval *interval*

undo dldp interval

Default

The interval for sending Advertisement packets is 5 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies Advertisement packets sending interval in the range of 1 to 100 seconds.

Usage guidelines

This command applies to all DLDP-enabled ports.

To enable DLDP to operate correctly, make sure the intervals for sending Advertisement packets configured on the two ends of a link are the same.

Examples

Set the interval for sending Advertisement packets to 20 seconds.

```
<Sysname> system-view
[Sysname] dldp interval 20
```

Related commands

display dldp

dldp port unidirectional-shutdown

Use **dldp port unidirectional-shutdown** to set the port shutdown mode for an interface.

Use **undo dldp port unidirectional-shutdown** to restore the default.

Syntax

dldp port unidirectional-shutdown { **auto** | **hybrid** | **manual** }

undo dldp port unidirectional-shutdown

Default

The global setting is used.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

auto: Specifies the auto mode. In this mode, when DLDP detects a unidirectional link, it shuts down the unidirectional port. When the link becomes bidirectional, DLDP brings up the port that was shut down.

hybrid: Specifies the hybrid mode. In this mode, when DLDP detects a unidirectional link, it shuts down the unidirectional port and stops link detection. To verify the link status, use the **undo shutdown** command to bring up the port. If the link becomes bidirectional, the port becomes bidirectional.

manual: Specifies the manual mode. In this mode, when DLDP detects a unidirectional link, it does not shut down the involved port. You must manually shut it down. To verify the link status, use the **undo shutdown** command to bring up the port. If the link becomes bidirectional, the port becomes bidirectional.

Usage guidelines

If DLDP detects a unidirectional link, you must troubleshoot the interface and cabling faults.

The port shutdown mode setting for an interface takes effect only on the current interface and has priority over the global port shutdown mode setting.

Examples

Set the port shutdown mode to **manual** for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dldp port unidirectional-shutdown manual
```

Related commands

display dldp

dldp unidirectional-shutdown

dldp unidirectional-shutdown

Use **dldp unidirectional-shutdown** to set the global port shutdown mode.

Use **undo dldp unidirectional-shutdown** to restore the default.

Syntax

dldp unidirectional-shutdown { **auto** | **hybrid** | **manual** }

undo dldp unidirectional-shutdown

Default

The global port shutdown mode is auto mode.

Views

System view

Predefined user roles

network-admin

Parameters

auto: Specifies the auto mode. In this mode, when DLDP detects a unidirectional link, it shuts down the unidirectional port. When the link becomes bidirectional, DLDP brings up the port that was shut down.

hybrid: Specifies the hybrid mode. In this mode, when DLDP detects a unidirectional link, it shuts down the unidirectional port and stops link detection. To verify the link status, use the **undo shutdown** command to bring up the port. If the link becomes bidirectional, the port becomes bidirectional.

manual: Specifies the manual mode. In this mode, when DLDP detects a unidirectional link, it does not shut down the involved port. You must manually shut it down. To verify the link status, use the **undo shutdown** command to bring up the port. If the link becomes bidirectional, the port becomes bidirectional.

Usage guidelines

If DLDP detects a unidirectional link, you must troubleshoot the interface and cabling faults.

The global port shutdown mode setting takes effect on all interfaces and has lower priority than the port shutdown mode setting for an interface.

Examples

Set the global port shutdown mode to manual mode.

```
<Sysname> system-view
[Sysname] dldp unidirectional-shutdown manual
```

Related commands

display dldp

dldp port unidirectional-shutdown

reset dldp statistics

Use **reset dldp statistics** to clear DLDP packet statistics.

Syntax

reset dldp statistics [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify this option, the command clears DLDP packet statistics for all interfaces.

Examples

Clear DLDP packet statistics for all interfaces.

```
<Sysname> reset dldp statistics
```

Related commands

display dldp statistics

Contents

RRPP commands

The following switch series do not support RRPP:

- S5110V2-SI.
- S5000V3-EI.
- S5000V5-EI.
- S5000E-X.
- S5000X-EI.
- WAS6000.

control-vlan

Use **control-vlan** to configure the primary control VLAN for an RRPP domain.

Use **undo control-vlan** to restore the default.

Syntax

control-vlan *vlan-id*

undo control-vlan

Default

No control VLANs exist in an RRPP domain.

Views

RRPP domain view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies the primary control VLAN by its ID in the range of 2 to 4093.

Usage guidelines

When you configure control VLANs for an RRPP domain, you only need to configure the primary control VLAN. The system automatically configures the secondary control VLAN. It uses the primary control VLAN ID plus 1 as the secondary control VLAN ID. For the control VLAN configuration to succeed, make sure the IDs of the two control VLANs are consecutive and have not been assigned yet.

Do not configure the default VLAN of a port accessing an RRPP ring as the control VLAN.

To ensure correct forwarding of RRPPDUs, do not enable QinQ or VLAN mapping on the control VLANs.

After you configure RRPP rings for an RRPP domain, you cannot delete or modify the primary control VLAN of the domain. To do so, use the **undo control-vlan** command.

Examples

Configure VLAN 100 as the primary control VLAN of RRPP domain 1 (assume that VLAN 100 and VLAN 101 have not been created yet).

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] control-vlan 100
```

display rrpp brief

Use **display rrpp brief** to display brief RRPP information.

Syntax

display rrpp brief

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display brief RRPP information.

```
<Sysname> display rrpp brief
 Flags for node mode: M –- Master, T -- Transit, E -- Edge, A -- Assistant-edge

 RRPP protocol status: Enabled

 Domain ID     : 1
 Control VLAN  : Primary 5, Secondary 6
 Protected VLAN: Reference instance 0 to 2, 4
 Hello timer   : 1 sec, Fail timer: 3 sec
 Linkup-Delay timer: 1 sec
  Ring  Ring   Node  Primary/Common            Secondary/Edge            Enable
  ID    level  mode  port                      port                      status
 ---------------------------------------------------------------------------
  1     1      M     GE1/0/1                   GE1/0/2                   Yes

 Domain ID     : 2
 Control VLAN  : Primary 10, Secondary 11
 Protected VLAN: Reference instance 0 to 2, 4
 Hello timer   : 1 sec, Fail timer: 3 sec
 Linkup-Delay timer: 1 sec
  Ring  Ring   Node  Primary/Common            Secondary/Edge            Enable
  ID    level  mode  port                      port                      status
 ---------------------------------------------------------------------------
  1     0      T     GE1/0/3                   GE1/0/4                   Yes
  2     1      E     GE1/0/3                   GE1/0/5                   Yes
                     GE1/0/4
```

Table 1 Command output

Field	Description
Flags for node mode	RRPP node mode: • **M**—Master node. • **T**—Transit node. • **E**—Edge node. • **A**—Assistant edge node.

Field	Description
RRPP protocol status	RRPP status: • **Enabled**—Globally enabled. • **Disabled**—Globally disabled.
Domain ID	RRPP domain ID.
Control VLAN	Primary and secondary control VLANs of the RRPP domain.
Protected VLAN	MSTIs corresponding to the VLANs protected by the RRPP domain. To view the VLAN-to-instance mappings, use the **display stp region-configuration** command (see *Layer 2—LAN Switching Command Reference*).
Hello timer	Hello timer value in seconds.
Fail timer	Fail timer value in seconds.
Linkup-Delay timer	Link-up delay timer value in seconds.
Ring ID	RRPP ring ID.
Ring level	RRPP ring level: • **0**—Primary ring. • **1**—Subring.
Primary/Common port	This field displays primary ports when the node mode is master node or transit node. This field displays common ports when the node mode is edge node or assistant edge node. A hyphen (-) appears when one of the following cases occurs: • The port is not configured on the ring. • The port is a member of a link aggregation group.
Secondary/Edge port	This field displays secondary ports when the node mode is master node or transit node. This field displays edge ports when the node mode is edge node or assistant edge node. A hyphen (-) appears when one of the following cases occurs: • The port is not configured on the ring. • The port is a member of a link aggregation group.
Enable status	RRPP ring status: • **Yes**—Enabled. • **No**—Disabled.

display rrpp ring-group

Use **display rrpp ring-group** to display the RRPP ring group configuration.

Syntax

display rrpp ring-group [*ring-group-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ring-group-id: Specifies an RRPP ring group by its ID in the range of 1 to 64 If you do not specify this argument, the command displays the configuration of all ring groups.

Usage guidelines

For an edge node RRPP ring group, this command also displays the subring sending Edge-Hello packets.

Examples

Display the configuration of all RRPP ring groups.

```
<Sysname> display rrpp ring-group
 Ring group 1:
  Domain 1 ring 1 to 3, 5
  Domain 2 ring 1 to 3, 5
  Domain 1 ring 1 is the sending ring

 Ring group 2:
  Domain 1 ring 4, 6 to 7
  Domain 2 ring 4, 6 to 7
```

Table 2 Command output

Field	Description
Ring group 1	RRPP ring group 1.
Domain 1 ring 1 to 3, 5	Subrings in the ring group, including rings 1, 2, 3, and 5 in RRPP domain 1.
Domain 1 ring 1 is the sending ring	The sending ring of the ring group is ring 1 in RRPP domain 1.

display rrpp statistics

Use **display rrpp statistics** to display RRPPDU statistics.

Syntax

display rrpp statistics domain *domain-id* [**ring** *ring-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

domain *domain-id*: Specifies an RRPP domain by its ID in the range of 1 to 128.

ring *ring-id*: Specifies an RRPP ring by its ID in the range of 1 to 128. If you do not specify this option, the command displays the RRPPDU statistics for all rings in the specified RRPP domain.

Usage guidelines

If a port belongs to more than one ring, this command collects and displays RRPPDU statistics of the port by ring.

When a ring transits from inactive status to active status, packet counting for the ring restarts.

Examples

Display RRPPDU statistics for all rings in RRPP domain 2.

```
<Sysname> display rrpp statistics domain 2
 Ring ID       : 1
 Ring level    : 0
 Node mode     : Master
 Active status : Yes
 Primary port  : GE1/0/3
  Direct Hello     Link     Common     Complete   Edge      Major     Total
                   down     flush FDB  flush FDB  hello     fault
 ---------------------------------------------------------------------------
  Out    16924     0        0          1          0         0         16925
  In     0         0        0          0          0         0         0
 Secondary port: GE1/0/4
  Direct Hello     Link     Common     Complete   Edge      Major     Total
                   down     flush FDB  flush FDB  hello     fault
 ---------------------------------------------------------------------------
  Out    0         0        0          0          0         0         0
  In     16878     0        0          1          0         0         16879

 Ring ID       : 2
 Ring level    : 1
 Node mode     : Edge
 Active status : No
 Common port   : GE1/0/3
  Direct Hello     Link     Common     Complete   Edge      Major     Total
                   down     flush FDB  flush FDB  hello     fault
 ---------------------------------------------------------------------------
  Out    0         0        0          0          0         0         0
  In     0         0        0          0          0         0         0
 Common port   : GE1/0/4
  Direct Hello     Link     Common     Complete   Edge      Major     Total
                   down     flush FDB  flush FDB  hello     fault
 ---------------------------------------------------------------------------
  Out    0         0        0          0          0         0         0
  In     0         0        0          0          0         0         0
 Edge port     : GE1/0/5
  Direct Hello     Link     Common     Complete   Edge      Major     Total
                   down     flush FDB  flush FDB  hello     fault
 ---------------------------------------------------------------------------
  Out    0         0        0          0          0         0         0
  In     0         0        0          0          0         0         0
```

Table 3 Command output

Field	Description
Ring ID	RRPP ring ID.
Ring level	RRPP ring level: • **0**—Primary ring. • **1**—Subring.
Node mode	Node mode: • Master node. • Transit node. • Edge node. • Assistant edge node.
Active status	RRPP ring status: • **Yes**—Active. • **No**—Inactive.
Primary port	The primary port field means the node mode is master node or transit node. A hyphen (-) appears when one of the following cases occurs: • The port is not configured on the ring. • The port is a member of a link aggregation group.
Secondary port	The secondary port field means the node mode is master node or transit node. A hyphen (-) appears when one of the following cases occurs: • The port is not configured on the ring. • The port is a member of a link aggregation group.
Common port	The common port field means the node mode is edge node or assistant edge node. A hyphen (-) appears when one of the following cases occurs: • The port is not configured on the ring. • The port is a member of a link aggregation group.
Edge port	The edge port field means the node mode is edge node or assistant edge node. A hyphen (-) appears when one of the following cases occurs: • The port is not configured on the ring. • The port is a member of a link aggregation group.
Packet direct	Packet transmission direction on the port: • **Out**—Packet sending direction. • **In**—Packet receiving direction.
Hello	Statistics of Hello packets received/sent on the port.
Link down	Statistics of Link-Down packets received/sent on the port.
Common flush FDB	Statistics of Common-Flush-FDB packets received/sent on the port.
Complete flush FDB	Statistics of Complete-Flush-FDB packets received/sent on the port.
Edge hello	Statistics of Edge-Hello packets received/sent on the port.
Major fault	Statistics of Major-Fault packets received/sent on the port.
Total	Total number of packets received/sent on the port. Only Hello, Link-Down, Common-Flush-FDB, Complete-Flush-FDB, Edge-Hello, and Major-Fault packets of RRPP are counted.

Related commands

reset rrpp statistics

display rrpp verbose

Use **display rrpp verbose** to display detailed RRPP information.

Syntax

display rrpp verbose domain *domain-id* [**ring** *ring-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

domain *domain-id*: Specifies an RRPP domain by its ID in the range of 1 to 128.

ring *ring-id*: Specifies an RRPP ring by its ID in the range of 1 to 128. If you do not specify this option, the command displays detailed information for all rings in the specified RRPP domain.

Examples

Display detailed information for all rings in RRPP domain 2.

```
<Sysname> display rrpp verbose domain 2
 Domain ID     : 2
 Control VLAN  : Primary 10, Secondary 11
 Protected VLAN: Reference instance 3, 5 to 7
 Hello timer   : 1 sec, Fail timer: 3 sec
 Linkup-Delay timer: 1 sec

 Ring ID       : 1
 Ring level    : 0
 Node mode     : Master
 Ring state    : Completed
 Enable status : Yes, Active status: Yes
 Primary port  : GE1/0/4                   Port status: UP
 Secondary port: GE1/0/5                   Port status: BLOCKED

 Ring ID       : 2
 Ring level    : 1
 Node mode     : Edge
 Ring state    : Unknown
 Enable status : No, Active status: No
 Common port   : GE1/0/4                   Port status: -
                 GE1/0/5                   Port status: -
 Edge port     : GE1/0/3                   Port status: -
```

Table 4 Command output

Field	Description
Domain ID	RRPP domain ID.
Control VLAN	Control VLANs of the RRPP domain: • **Primary**—Primary control VLAN. • **Secondary**—Secondary control VLAN.
Protected VLAN	MSTIs corresponding to the VLANs protected by the RRPP domain. To view the VLAN-to-instance mappings, use the **`display stp region-configuration`** command (see *Layer 2—LAN Switching Command Reference*).
Hello timer	Hello timer value in seconds.
Fail timer	Fail timer value in seconds.
Linkup-Delay timer	Link-up delay timer value in seconds.
Ring ID	RRPP ring ID.
Ring level	RRPP ring level: • **0**—Primary ring. • **1**—Subring.
Node mode	Node mode: • Master node. • Transit node. • Edge node. • Assistant edge node.

Ring state	RRPP ring state:
	• Possible states on the master node:
	  ○ **Completed**—The ring is healthy.
	  ○ **Failed**—The ring is not closed.
	  ○ **Unknown**—The RRPP domain is disabled.
	• Possible states on a transit node or edge node:
	  ○ **LinkUp**—All ports on the node are up.
	  ○ **LinkDown**—At least one port on the node is down.
	  ○ **PreForward**—A port on the node is blocked.
	  ○ **Unknown**—The RRPP domain is disabled.
	• Possible states on an assistant edge node:
	  ○ **LinkUp**—All ports on the node are up.
	  ○ **LinkDown**—At least one port on the node is down.
	  ○ **PreForward**—A port on the node is blocked.
	  ○ **LinkUpNotify**—The node does not receive Edge-Hello packets in LinkUp state.
	  ○ **LinkDnNotify**—The node does not receive Edge-Hello packets in LinkDown state.
	  ○ **PreForwardNotify**—The port on the directly connected edge node comes up, or the assistant edge node does not receive Edge-Hello packets in PreForward state.
	  ○ **Unknown**—The RRPP domain is disabled.
	If the ring is not enabled on the device operating as the master node or the device is not the master node of the ring, a hyphen (-) is displayed.

Enable status	RRPP ring status: • **Yes**—Enabled. • **No**—Disabled.

Field	Description
Active status	RRPP ring status: • **Yes**—Active. • **No**—Inactive. An RRPP ring can be active only when RRPP and the RRPP ring are both enabled. This field also helps you identify whether RRPP is enabled.
Primary port	The primary port field means the node mode is master node or transit node. A hyphen (-) appears when one of the following cases occurs: • The port is not configured on the ring. • The port is a member of a link aggregation group.
Secondary port	The secondary port field means the node mode is master node or transit node. A hyphen (-) appears when one of the following cases occurs: • The port is not configured on the ring. • The port is a member of a link aggregation group.
Common port	The common port field means the node mode is edge node or assistant edge node. A hyphen (-) appears when one of the following cases occurs: • The port is not configured on the ring. • The port is a member of a link aggregation group.
Edge port	The edge port field means the node mode is edge node or assistant edge node. A hyphen (-) appears when one of the following cases occurs: • The port is not configured on the ring. • The port is a member of a link aggregation group.
Port status	Port status: Down, up, or blocked. A hyphen (-) appears when one of the following cases occurs: • The ring is inactive. • The port is not configured on the ring. • The port is a member of a link aggregation group.

domain ring

Use **domain ring** to configure subrings for an RRPP ring group.

Use **undo domain ring** to remove subrings from the RRPP ring group.

Syntax

domain *domain-id* **ring** *ring-id-list*

undo domain *domain-id* [**ring** *ring-id-list*]

Default

No subrings exist in an RRPP ring group.

Views

RRPP ring group view

Predefined user roles

network-admin

Parameters

domain-id: Specifies an RRPP domain by its ID in the range of 1 to 128.

ring *ring-id-list*: Specifies a space-separated list of up to 10 RRPP subring ID items. Each item specifies an RRPP subring ID or a range of RRPP subring IDs. The value range for RRPP subring IDs is 1 to 128. If you do not specify this option, the command removes all subrings from the ring group in the specified domain.

Usage guidelines

Follow these guidelines when you configure an RRPP ring group on the edge node and the assistant edge node:

- When you assign an active ring to a ring group, assign it on the assistant edge node first and then on the edge node.
- To remove an active ring from a ring group, remove it on the edge node first and then on the assistant edge node.
- To remove a ring group, remove it on the edge node first and then on the assistant edge node.
- When you activate rings in a ring group, activate them on the edge node first and then on the assistant edge node.
- When you deactivate rings in a ring group, deactivate them on the assistant edge node first and then on the edge node.

If you do not follow these guidelines, the assistant edge node might fail to receive Edge-Hello packets and consider the primary ring failed even if it did not.

Examples

Create RRPP ring group 1, and add subrings 1, 2, 3, and 5 to domain 1 and domain 2.

```
<Sysname> system-view
[Sysname] rrpp ring-group 1
[Sysname-ring-group1] domain 1 ring 1 to 3 5
[Sysname-ring-group1] domain 2 ring 1 to 3 5
```

Related commands

display rrpp ring-group

rrpp ring-group

linkup-delay-timer

Use **linkup-delay-timer** to set the link-up delay timer.

Use **undo linkup-delay-timer** to restore the default.

Syntax

linkup-delay-timer *delay-time* [**distribute**]

undo linkup-delay-timer

Default

The link-up delay timer is 0 seconds, and the **distribute** keyword is not specified.

Views

RRPP domain view

Predefined user roles

network-admin

Parameters

delay-time: Specifies the link-up delay timer in the range of 0 to 30 seconds.

distribute: Enables all nodes in the RRPP domain to learn the link-up delay timer value.

Usage guidelines

The link-up delay timer prevents frequent switchover of RRPP traffic forwarding paths caused by unstable RRPP port states.

You can configure this command on any node in an RRPP domain, but this command can take effect only on the master node.

If you specify the **distribute** keyword in an RRPP network implementing load balancing, you must configure the link-up delay timer for each RRPP domain for the timer to take effect. If you set different timer values for different RRPP domains, the smallest timer value takes effect.

If the **distribute** keyword is not specified, the link-up delay timer value cannot be greater than the Fail timer value minus twice the Hello timer value.

Examples

Set the link-up delay timer to 10 seconds for RRPP domain 1.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] linkup-delay-timer 10
```

Related commands

timer

protected-vlan

Use **protected-vlan** to configure the protected VLANs for an RRPP domain.

Use **undo protected-vlan** to remove the protected VLANs from an RRPP domain.

Syntax

protected-vlan reference-instance *instance-id-list*

undo protected-vlan [**reference-instance** *instance-id-list*]

Default

No protected VLANs exist in an RRPP domain.

Views

RRPP domain view

Predefined user roles

network-admin

Parameters

reference-instance *instance-id-list*: Specifies the Multiple Spanning Tree Instances (MSTIs) you want to reference in the form of *instance-id-list* = { *instance-id* [**to** *instance-id*] }&<1-10>. The *instance-id* argument is an MSTI ID in the range of 0 to 4094. You can specify up to 10 MSTI IDs or ID ranges. You can use the **display stp region-configuration** command to display the VLAN-to-instance mappings. If you do not specify this option, the command removes all MSTIs referenced by the RRPP domain.

Usage guidelines

You can delete or modify the protected VLANs configured for an RRPP domain before and after you configure rings for the domain. However, after you configure rings for the RRPP domain, you cannot delete configurations of all the protected VLANs configured for the domain.

When the VLAN-to-instance mappings change, the protected VLANs of an RRPP domain also change.

Examples

Map VLANs 1 through 30 to MSTI 1, and activate the MST region configuration. Configure VLAN 100 as the control VLAN of RRPP domain 1. Configure VLANs mapped to MSTI 1 as the primary control VLANs of RRPP domain 1.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] instance 1 vlan 1 to 30
[Sysname-mst-region] active region-configuration
[Sysname-mst-region] quit
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] control-vlan 100
[Sysname-rrpp-domain1] protected-vlan reference-instance 1
```

Related commands

display stp region-configuration (*Layer 2—LAN Switching Command Reference*)

rrpp domain

reset rrpp statistics

Use **reset rrpp statistics** to clear RRPPDU statistics.

Syntax

reset rrpp statistics domain *domain-id* [**ring** *ring-id*]

Views

User view

Predefined user roles

network-admin

Parameters

domain *domain-id*: Specifies an RRPP domain by its ID in the range of 1 to 128.

ring *ring-id*: Specifies an RRPP ring by its ID in the range of 1 to 128. If you do not specify this option, the command clears RRPPDU statistics of all RRPP rings in the specified RRPP domain.

Examples

Clear the RRPPDU statistics of ring 10 in RRPP domain 1.

```
<Sysname> reset rrpp statistics domain 1 ring 10
```

Related commands

display rrpp statistics

ring

Use **ring** to configure the node mode of the device, the role of the specified RRPP port, and the level of the RRPP ring.

Use **undo ring** to delete the RRPP ring.

Syntax

ring *ring-id* **node-mode** { { **master** | **transit** } [**primary-port** *interface-type interface-number*] [**secondary-port** *interface-type interface-number*] **level** *level-value* | { **assistant-edge** | **edge** } [**edge-port** *interface-type interface-number*] }

undo ring *ring-id*

Default

The device is not a node of the RRPP ring.

Views

RRPP domain view

Predefined user roles

network-admin

Parameters

ring-id: Specifies an RRPP ring by its ID in the range of 1 to 128.

master: Specifies the device as the master node of the RRPP ring.

transit: Specifies the device as the transit node of the RRPP ring.

primary-port: Specifies the port as a primary port.

interface-type interface-number: Specifies a port by its type and number.

secondary-port: Specifies the port as a secondary port.

level *level-value*: Specifies an RRPP ring level, 0 for the primary ring and 1 for the subring.

assistant-edge: Specifies the device as the assistant edge node of the RRPP ring.

edge: Specifies the device as the edge node of the RRPP ring.

edge-port: Specifies the edge port for the node.

Usage guidelines

The ID of an RRPP ring in a domain must be unique.

When an RRPP ring is activated, you cannot configure its RRPP ports.

When you configure the edge node and the assistant edge node, first configure the primary ring, and then the subrings.

The node mode, RRPP port role, and ring level settings of an RRPP ring cannot be modified after they are configured. To modify the settings, first remove the current settings.

Remove all subring configurations before you delete the primary ring configuration of the edge node or the assistant edge node. However, an active RRPP ring cannot be deleted.

When RRPP is enabled on a device, you must disable the RRPP ring before you can delete it. When RRPP is disabled on the device, you can directly delete the RRPP ring, as well as the setting of the **ring enable** command.

Do not assign a port to both an aggregation group and an RRPP ring. If you do so, the port does not take effect on the RRPP ring.

Examples

Specify the device as the master node of primary ring 10 in RRPP domain 1. Specify GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
<Sysname> system-view
[Sysname] rrpp domain 1
```

```
[Sysname-rrpp-domain1] control-vlan 100
[Sysname-rrpp-domain1] protected-vlan reference-instance 0 1 2
[Sysname-rrpp-domain1] ring 10 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
```

Specify the device as the transit node of primary ring 10 in RRPP domain 1. Specify GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Specify the device as the edge node of subring 20 in RRPP domain 1, and specify GigabitEthernet 1/0/3 as the edge port.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] control-vlan 100
[Sysname-rrpp-domain1] protected-vlan reference-instance 0 1 2
[Sysname-rrpp-domain1] ring 10 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[Sysname-rrpp-domain1] ring 20 node-mode edge edge-port gigabitethernet 1/0/3
```

Related commands

ring enable

ring enable

Use **ring enable** to enable an RRPP ring.

Use **undo ring enable** to disable the RRPP ring.

Syntax

ring *ring-id* **enable**

undo ring *ring-id* **enable**

Default

An RRPP ring is disabled.

Views

RRPP domain view

Predefined user roles

network-admin

Parameters

ring-id: Specifies an RRPP ring by its ID in the range of 1 to 128.

Usage guidelines

To activate an RRPP ring, you must enable RRPP and the RRPP ring.

Before you enable subrings on a device, you must enable the primary ring. Before you disable the primary ring on the device, you must disable all subrings. Otherwise, the system displays error prompts.

Examples

Enable RRPP ring 10 in RRPP domain 1.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] control-vlan 100
[Sysname-rrpp-domain1] protected-vlan reference-instance 0 1 2
```

```
[Sysname-rrpp-domain1] ring 10 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[Sysname-rrpp-domain1] ring 10 enable
```

Related commands

rrpp enable

rrpp domain

Use **rrpp domain** to create an RRPP domain and enter its view, or enter the view of an existing RRPP domain.

Use **undo rrpp domain** to remove an RRPP domain.

Syntax

rrpp domain *domain-id*

undo rrpp domain *domain-id*

Default

No RRPP domains exist.

Views

System view

Predefined user roles

network-admin

Parameters

domain-id: Specifies an RRPP domain by its ID in the range of 1 to 128.

Usage guidelines

When you delete an RRPP domain, configurations of the control VLANs and protected VLANs are deleted at the same time.

To delete an RRPP domain successfully, make sure it has no RRPP rings.

Examples

Create RRPP domain 1, and enter RRPP domain 1 view.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1]
```

Related commands

control-vlan

protected-vlan

rrpp enable

Use **rrpp enable** to enable RRPP.

Use **undo rrpp enable** to disable RRPP.

Syntax

rrpp enable

undo rrpp enable

Default

RRPP is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

To activate an RRPP domain, enable RRPP and the RRPP rings for the RRPP domain.

Examples

Enable RRPP.

```
<Sysname> system-view
[Sysname] rrpp enable
```

Related commands

ring enable

rrpp ring-group

Use **rrpp ring-group** to create an RRPP ring group and enter its view, or enter the view of an existing RRPP ring group.

Use **undo rrpp ring-group** to remove an RRPP ring group.

Syntax

rrpp ring-group *ring-group-id*

undo rrpp ring-group *ring-group-id*

Default

No RRPP ring groups exist.

Views

System view

Predefined user roles

network-admin

Parameters

ring-group-id: Specifies an RRPP ring group ID in the range of 1 to 64.

Usage guidelines

When you remove a ring group, remove it on the edge node first and then on the assistant edge node. Otherwise, the assistant edge node might fail to receive Edge-Hello packets and consider the primary ring failed even if it is not.

After a ring group is removed, all subrings in the ring group do not belong to any ring group.

Examples

Create RRPP ring group 1 and enter its view.

```
<Sysname> system-view
[Sysname] rrpp ring-group 1
```

```
[Sysname-ring-group1]
```

Related commands

display rrpp ring-group

domain ring

snmp-agent trap enable rrpp

Use **snmp-agent trap enable rrpp** to enable SNMP notifications for RRPP.

Use **undo snmp-agent trap enable rrpp** to disable SNMP notifications for RRPP.

Syntax

snmp-agent trap enable rrpp [**major-fault** | **multi-master** | **ring-fail** | **ring-recover**] *

undo snmp-agent trap enable rrpp [**major-fault** | **multi-master** | **ring-fail** | **ring-recover**] *

Default

SNMP notifications for RRPP are disabled.

Views

System view

Predefined user roles

network-admin

Parameters

major-fault: Generates notifications when an SRPT between the assistant edge node and edge node is disconnected.

multi-master: Generates notifications when multiple master nodes are configured for the RRPP ring.

ring-fail: Generates notifications when the state of the RRPP ring changes from Health to Disconnect.

ring-recover: Generates notifications when the state of the RRPP ring changes from Disconnect to Health.

Usage guidelines

To report critical RRPP events to an NMS, enable SNMP notifications for RRPP. For RRPP event notifications to be sent correctly, you must also configure SNMP on the device. For more information about SNMP configuration, see the network management and monitoring configuration guide for the device.

If you do not specify any keyword, this command enables or disables all SNMP notifications for RRPP.

Examples

Generate notifications when the state of the RRPP ring changes from Disconnect to Health.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable rrpp ring-recover
```

timer

Use **timer** to set the Hello timer and the Fail timer.

Use **undo timer** to restore the default.

Syntax

timer hello-timer *hello-value* **fail-timer** *fail-value*

undo timer

Default

The Hello timer is 1 second and the Fail timer is 3 seconds.

Views

RRPP domain view

Predefined user roles

network-admin

Parameters

hello-timer *hello-value*: Specifies the Hello timer in the range of 1 to 10 seconds.

fail-timer *fail-value*: Specifies the Fail timer in the range of 3 to 30 seconds.

Usage guidelines

The Fail timer must be greater than or equal to three times the Hello timer.

Examples

Set the Hello timer to 2 seconds and the Fail timer to 7 seconds for RRPP domain 1.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] timer hello-timer 2 fail-timer 7
```

Contents

ERPS commands

control-vlan

Use **control-vlan** to configure the control VLAN for an ERPS instance.

Use **undo control-vlan** to restore the default.

Syntax

control-vlan *vlan-id*

undo control-vlan

Default

An ERPS instance does not have control VLANs.

Views

ERPS instance view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies the control VLAN by its ID in the range of 2 to 4094.

Usage guidelines

The control VLAN must be a VLAN that has not been created on the device.

Examples

Configure VLAN 100 as the control VLAN for instance 1 of ERPS ring 1.

```
<Sysname> system-view
[Sysname] erps ring 1
[Sysname-erps-ring1] instance 1
[Sysname-erps-ring1-inst1] control-vlan 100
```

Related commands

instance

display erps

Use **display erps** to display brief ERPS ring information.

Syntax

display erps

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display brief ERPS ring information.

```
<Sysname> display erps
ERPS protocol status: Enabled
ERPS tcn-propagation: Enabled
Flags: R -- RPL, F -- Faulty, B -- Blocked,
       FS -- Forced switch, MS -- Manual switch
Ring   Instance   NodeRole   NodeState    Port0     Port1    Status
--------------------------------------------------------------------------
1      1          Owner      Idle         R,B               Enabled
1      2          Normal     Idle                           Disabled
2      1          Owner      Idle         R,B               Enabled
2      2          Normal     Idle                           Disabled
```

Table 1 Command output

Field	Description
ERPS protocol status	ERPS state: • **Enabled**—Globally enabled. • **Disabled**—Globally disabled.
ERPS tcn-propagation	State of the flush packet transparent transmission feature: • **Enabled**—Globally enabled. • **Disabled**—Globally disabled.
Ring	ERPS ring ID.
Instance	ERPS instance ID.
NodeRole	Node type: • Owner. • Neighbor. • Interconnection. • Normal.
NodeState	Node state: • **Idle**—The ERPS ring enters the idle state after initialization. • **Protection**—The ERPS ring enters the protection state when a link fails. • **MS**—Manual switching mode. • **FS**—Forced switching mode. • **Pending**—Transient mode between any two states. • **-**—ERPS is disabled for the ERPS instance or disabled globally.
Port0	State of port 0: • **R**—The port is an RPL port. • **B**—The port is blocked. • **F**—The port is unavailable and the link for the port is faulty. • **FS**—The port is in FS mode. • **MS**—The port is in MS mode. • **-**—The port is not an ERPS ring member port. If this field is blank, the port is not in any of the previous states.

Field	Description
Port1	State of port 1: • **R**—The port is an RPL port. • **B**—The port is blocked. • **F**—The port is unavailable and the link for the port is faulty. • **FS**—The port is in FS mode. • **MS**—The port is in MS mode. • **-**—The port is not an ERPS ring member port. If this field is blank, the port is not in any of the previous states.
Status	State of the ERPS instance: • Enabled. • Disabled.

display erps detail

Use **display erps detail** to display detailed ERPS ring information.

Syntax

display erps detail ring *ring-id* [**instance** *instance-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ring *ring-id*: Specifies an ERPS ring by its ID in the range of 1 to 255.

instance *instance-id*: Specifies an ERPS instance by its ID in the range of 1 to 64. If you do not specify this option, this command displays detailed information about all instances for the ERPS ring.

Examples

Display detailed information about instance 1 of ERPS ring 1.

```
<Sysname> display erps detail ring 1 instance 1
Ring ID                : 1
Port0                  : GigabitEthernet1/0/1
Port1                  : GigabitEthernet1/0/2
Subring                : Yes
Default MAC            : Yes

Instance ID            : 1
Node role              : Owner
Node state             : Idle
Connect (ring/instance): (1/2), (2/3)
Control VLAN           : 100
Protected VLAN         : Reference-instance 0 to 2
Guard timer            : 500 ms
```

```
Hold-off timer         : 1 sec
WTR timer              : 5 min
Revertive operation    : Non-revertive
Enable status          : Yes, Active Status : Yes
R-APS level            : 1
Port                   PortRole              PortStatus
--------------------------------------------------------------------
Port0                  RPL                   Block
Port1                  Non-RPL               Up
```

Display detailed information about all instances of ERPS ring 1.

```
<Sysname> display erps detail ring 1
Ring ID               : 1
Port0                 : GigabitEthernet1/0/1
Port1                 : GigabitEthernet1/0/2
Subring               : Yes
Default MAC           : Yes

Instance ID           : 1
Node role             : Owner
Node state            : Idle
Connect(ring/instance): (1/2), (2/3)
Control VLAN          : 100
Protected VLAN        : Reference-instance 0 to 2
Guard timer           : 500 ms
Hold-off timer        : 1 sec
WTR timer             : 5 min
Revertive operation   : Non-revertive
Enable status         : Yes, Active Status : Yes
R-APS level           : 1
Port                  PortRole              PortStatus
--------------------------------------------------------------------
Port0                 RPL                   Block
Port1                 Non-RPL               Up

Instance ID           : 2
Node role             : Neighbor
Node state            : Idle
Connect(ring/instance): (1/2), (2/3)
Control VLAN          : 200
Protected VLAN        : Reference-instance 3
Guard timer           : 500 ms
Hold-off timer        : 1 sec
Wtr timer             : 5 min
Revertive operation   : Non-revertive
Enable status         : Yes, Active Status : Yes
R-APS level           : 1
Port                  PortRole              PortStatus
--------------------------------------------------------------------
```

```
Port0                RPL                  Block
Port1                Non-RPL              Up
```

Table 2 Command output

Field	Description
Port0	ERPS ring member port 0.
Port1	ERPS ring member port 1.
Subring	ERPS subring status: • **Yes**—The ring is a subring. • **No**—The ring is not a subring.
Default MAC	Default MAC address status: • **Yes**—The last byte is 1 in the destination MAC address of R-APS packets. • **No**—The last byte is the ring ID in the destination MAC address of R-APS packets.
Node role	Node type: • Owner. • Neighbor. • Interconnection. • Normal.
Node state	Node state: • **Idle**—The ERPS ring enters the idle status after initialization. • **Protection**—The ERPS ring enters the protection state when a link fails. • **MS**—Manual switching mode. • **FS**—Forced switching mode. • **Pending**—Transient mode between any two states. • **-**—ERPS is disabled for the ERPS instance or disabled globally.
Connect(ring/instance)	Ring or instance associated with the ERPS instance.
Control VLAN	Control VLAN of the ERPS instance.
Protected VLAN	List of VLANs protected by the ERPS instance, which are represented by MSTIs. To view the mapping between MSTIs and VLANs, use the **`display stp region-configuration`** command.
Guard timer	Guard timer in milliseconds.
Hold-off timer	Hold-off timer in milliseconds.
WTR timer	WTR timer in minutes.
Revertive operation	Revertive mode: • Non-revertive. • Revertive.
Enable status	ERPS status for the instance: • **Yes**—Enabled. • **No**—Disabled.
Active Status	Global ERPS status and ERPS status for the instance: • **Yes**—Enabled. • **No**—Disabled.
R-APS level	Level of the R-APS packets.

Field	Description
Port	ERPS ring member port.
PortRole	Port role: • **RPL**—The port is an RPL port. • **Non-RPL**—The port is not an RPL port.
Port Status	Port status: • **Block**—The port is blocked. • **Up**—The link is up. • **Down**—The link is down.

display erps statistics

Use **display erps statistics** to display ERPS packet statistics.

Syntax

display erps statistics *ring-id* [**instance** *instance-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ring *ring-id*: Specifies an ERPS ring by its ID in the range of 1 to 255.

instance *instance-id*: Specifies an ERPS instance by its ID in the range of 1 to 64. If you do not specify this option, this command displays packet statistics for all instances of the ERPS ring.

Examples

Display packet statistics for all instances of ERPS ring 1.

```
<Sysname> display erps statistics ring 1
  Statistics for ERPS ring 1 instance 1:
  R-APS      Port0(Tx/Rx)             Port1(Tx/Rx)
  --------------------------------------------------
  NR         1/1                      1/1
  NR,RB      0/1                      0/1
  SF         1/0                      1/0
  MS         0/0                      0/0
  FS         0/0                      0/0
  Total      2/2                      2/2

  Statistics for ERPS ring 1 instance 2:
  R-APS      Port0(Tx/Rx)             Port1(Tx/Rx)
  --------------------------------------------------
  NR         1/1                      1/1
  NR,RB      0/1                      0/1
  SF         1/0                      1/0
  MS         0/0                      0/0
```

```
FS          0/0                     0/0
Total       2/2                     2/2
```

Table 3 Command output

Field	Description
R-APS	Packet type.
Port0(Tx/Rx)	Packet statistics for port 0: • **Tx**—Transmitted packets. • **Rx**—Received packets.
Port1(Tx/Rx)	Packet statistics for port 1: • **Tx**—Transmitted packets. • **Rx**—Received packets.

erps clear

Use **erps clear** to remove the MS mode and FS mode settings for an ERPS ring.

Syntax

erps clear *ring-id* **instance** *instance-id*

Views

System view

Predefined user roles

network-admin

Parameters

ring *ring-id*: Specifies an ERPS ring by its ID in the range of 1 to 255.

instance *instance-id*: Specifies an ERPS instance by its ID in the range of 1 to 64.

Usage guidelines

After you configure this command, the owner node can ignore the WTR timer and immediately switch traffic to the recovered link upon link recovery.

This command also switches an ERPS ring in non-revertive mode to revertive mode.

Examples

Remove the MS mode and FS mode settings for instance 1 on ERPS ring 1.

```
<Sysname> system-view
[Sysname] erps clear ring 1 instance 1
```

erps enable

Use **erps enable** to enable ERPS globally.

Use **undo erps enable** to restore the default.

Syntax

erps enable

undo erps enable

Default

ERPS is disabled globally.

Views

System view

Predefined user roles

network-admin

Examples

Enable ERPS.

```
<Sysname> system-view
[Sysname] erps enable
```

erps ring

Use **erps ring** to create an ERPS ring.

Use **undo erps ring** to delete an ERPS ring.

Syntax

erps ring *ring-id*

undo erps ring *ring-id*

Default

No ERPS rings exist.

Views

System view

Predefined user roles

network-admin

Parameters

ring *ring-id*: Specifies an ERPS ring by its ID in the range of 1 to 255.

Usage guideline

To delete an ERPS ring successfully, delete all ERPS instances on the ring first.

Examples

Create ERPS ring 1.

```
<Sysname> system-view
[Sysname] erps ring 1
[Sysname-erps-ring1]
```

Related commands

instance

erps switch

Use **erps switch** to configure the switching mode for an ERPS ring.

Syntax

erps switch { **force** | **manual** } **ring** *ring-id* **instance** *instance-id* { **port0** | **port1** }

Views

System view

Predefined user roles

network-admin

Parameters

force: Configures the forced switching mode.

manual: Configures the manual switching mode.

port0: Specifies the ERPS ring member port 0.

port1: Specifies the ERPS ring member port 1.

ring *ring-id*: Specifies an ERPS ring by its ID in the range of 1 to 255.

instance *instance-id*: Specifies an ERPS instance by its ID in the range of 1 to 64.

Examples

Configure the forced switching mode for port 1 of instance 1 on ERPS ring 1.

```
<Sysname> system-view
[Sysname] erps switch force ring 1 instance 1 port0
```

erps tcn-propagation

Use **erps tcn-propagation** to enable flush packet transparent transmission for an interconnection node.

Use **undo erps tcn-propagation** to restore the default.

Syntax

erps tcn-propagation

undo erps tcn-propagation

Default

Flush packet transparent transmission is disabled for an interconnection node.

Views

System view

Predefined user roles

network-admin

Usage guideline

This command must be used together with the **sub-ring connect** command.

Examples

Enable flush packet transparent transmission for the interconnection node.

```
<Sysname> system-view
[Sysname] erps tcn-propagation
```

Related commands

sub-ring connect

instance

Use **instance** to create an instance for an ERPS ring.

Use **undo instance** to delete an instance from an ERPS ring.

Syntax

instance *instance-id*

undo instance *instance-id*

Default

An ERPS ring does not have instances.

Views

ERPS ring view

Predefined user roles

network-admin

Parameters

instance *instance-id*: Specifies an ERPS instance by its ID in the range of 1 to 64.

Usage guidelines

You can create multiple instances for an ERPS ring. Each instance has its own protected VLAN, control VLAN, and RPL owner. Each instance maintains its own state machine and data. You can locate an ERPS instance by its ring ID and VLAN ID.

Examples

Create instance 1 for ERPS ring 1.

```
<Sysname> system-view
[Sysname] erps ring 1
[Sysname-erps-ring1] instance 1
[Sysname-erps-ring1-inst1]
```

Related commands

erps ring

instance enable

Use **instance enable** to enable ERPS for an ERPS instance.

Use **undo instance enable** to disable ERPS for an ERPS instance.

Syntax

instance enable

undo instance enable

Default

ERPS is disabled for ERPS instances.

Views

ERPS instance view

Predefined user roles

network-admin

Examples

Create ERPS instance 1 and enable ERPS for the instance.

```
<Sysname> system-view
[Sysname] erps ring 1
[Sysname-erps-ring1] instance 1
[Sysname-erps-ring1-inst1] control-vlan 100
[Sysname-erps-ring1-inst1] protected-vlan reference-instance 0 1 2
[Sysname-erps-ring1-inst1] instance enable
```

Related commands

instance

node-role

Use **node-role** to configure the role for an ERPS node.

Use **undo node-role** to restore the default.

Syntax

node-role { { **owner** | **neighbor** } **rpl** | **interconnection** } { **port0** | **port1** }

undo node-role

Default

An ERPS node is a normal node.

Views

ERPS instance view

Predefined user roles

network-admin

Parameters

owner: Configures the owner node.

neighbor: Configures the neighbor node.

interconnection: Configures the interconnection node for connecting the major ring and subring.

Usage guidelines

For the owner node to work correctly, you must configure only one owner node for an ERPS ring.

You can configure an interconnection node only for a subring.

Examples

Configure instance 1 of ERPS ring 1 as an RPL owner node and configure port 0 as an RPL port.

```
<Sysname> system-view
[Sysname] erps ring 1
[Sysname-erps-ring1] instance 1
```

```
[Sysname-erps-ring1-inst1] node-role owner rpl port0
```

port erps track

Use **port erps track** to associate an ERPS ring member port with a track entry.

Use **undo port erps track** to remove the association between an ERPS ring member port and a track entry.

Syntax

port erps ring *ring-id* **instance** *instance-id* **track** *track-entry-index*

undo port erps ring *ring-id* **instance** *instance-id* **track**

Default

An ERPS ring member port is not associated with track entries.

Views

Interface view

Predefined user roles

network-admin

Parameters

ring *ring-id*: Specifies an ERPS ring by its ID in the range of 1 to 255.

instance *instance-id*: Specifies an ERPS instance by its ID in the range of 1 to 64.

track-entry-index: Specifies a track entry by its ID in the range of 1 to 1024. For more information about specifying the track entry ID, see the **track cfd** command in "Track commands."

Usage guidelines

An ERPS ring member port collaborates with link detection protocols through track entries. ERPS supports only the CC feature of CFD to implement link detection.

Examples

Associate a track entry with GigabitEthernet 1/0/1 on the RPL owner node in instance 1 of ERPS ring 1.

```
<Sysname> system-view
[Sysname] erps ring 1
[Sysname-erps-ring1] port0 interface gigabitethernet 1/0/1
[Sysname-erps-ring1] instance 1
[Sysname-erps-ring1-inst1] node-role owner rpl port0
[Sysname-erps-ring1-inst1] quit
[Sysname-erps-ring1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port erps ring 1 instance 1 track 3
```

Related commands

track cfd

port0

Use **port0** to specify the first member port for an ERPS ring.

Use **undo port0** to restore the default.

Syntax

port0 interface *interface-type interface-number*

undo port0

Default

No member ports exist in an ERPS ring.

Views

ERPS ring view

Predefined user roles

network-admin

Usage guidelines

Do not assign an interface to both an aggregation group and an ERPS ring. If you do so, the interface does not take effect on the ERPS ring and cannot be displayed by using the **display erps detail** command.

Parameters

interface *interface-type interface-number*: Specifies a Layer 2 Ethernet interface or a Layer 2 aggregate interface by its type and number.

Examples

Specify GigabitEthernet 1/0/1 as the first member port for ERPS ring 1.

```
<Sysname> system-view
[Sysname] erps ring 1
[Sysname-erps-ring1] port0 interface gigabitethernet 1/0/1
```

port1

Use **port1** to specify the second member port for an ERPS ring.

Use **undo port1** to restore the default.

Syntax

port1 interface *interface-type interface-number*

undo port1

Default

No member ports exist in an ERPS ring.

Views

ERPS ring view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a Layer 2 Ethernet interface or a Layer 2 aggregate interface by its type and number.

Usage guidelines

Do not assign an interface to both an aggregation group and an ERPS ring. If you do so, the interface does not take effect on the ERPS ring and cannot be displayed by using the **display erps detail** command.

Examples

Specify GigabitEthernet 1/0/2 as the second member port for ERPS ring 1.

```
<Sysname> system-view
[Sysname] erps ring 1
[Sysname-erps-ring1] port1 interface gigabitethernet 1/0/2
```

protected-vlan

Use **protected-vlan** to configure protected VLANs for an ERPS instance.

Use **undo protected-vlan** to delete protected VLANs for an ERPS instance.

Syntax

protected-vlan reference-instance *instance-id-list*

undo protected-vlan [**reference-instance** *instance-id-list*]

Default

No protected VLANs exist in an ERPS instance.

Views

ERPS instance view

Predefined user roles

network-admin

Parameters

instance-id-list: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* **to** *instance-id2*. The value for *instance-id2* must be greater than or equal to the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094. The value 0 indicates CIST. You can use the **display stp region-configuration** command to display the VLAN-to-instance mappings. In PVST mode, the system automatically maps VLANs to MSTIs.

Usage guidelines

If you do not specify the **reference-instance** *instance-id-list* option, the **undo protected-vlan** command deletes all mappings between MSTIs and VLANs in the ERPS instance. The protected VLANs change if the mappings between the MSTIs and VLANs change.

Examples

Configure the protected VLANs for instance 1 of ERPS ring 1.

```
<Sysname> system-view
[Sysname] erps ring 1
[Sysname-erps-ring1] instance 1
[Sysname-erps-ring1-inst1] protected-vlan reference-instance 0 1 2
```

Related commands

display stp region-configuration

r-aps level

Use **r-aps level** to configure the level for R-APS packets.

Use **undo r-aps level** to restore the default.

Syntax

r-aps level *level-value*

undo r-aps level

Default

The R-APS packet level is 7.

Views

ERPS instance view

Predefined user roles

network-admin

Parameters

level-value: Specifies the R-APS packet level in the range of 0 to 7.

Usage guidelines

The R-APS packet level must be the same for all nodes in an instance of an ERPS ring.

Examples

Configure the R-APS packet level as 1 for instance 1 of ERPS ring 1.

```
<Sysname> system-view
[Sysname] erps ring 1
[Sysname-erps-ring1] instance 1
[Sysname-erps-ring1-inst1] r-aps level 1
```

r-aps ring-mac

Use **r-aps ring-mac** to configure the ring ID as the last byte of the destination MAC address for R-APS packets.

Use **undo r-aps ring-mac** to restore the default.

Syntax

r-aps ring-mac

undo r-aps ring-mac

Default

The last byte of the destination MAC address is 1 for the R-APS packets.

Views

ERPS ring view

Predefined user roles

network-admin

Examples

Configure the ID of ERPS ring 2 as the last byte of the destination MAC address for R-APS packets.

```
<Sysname> system-view
[Sysname] erps ring 2
[Sysname-erps-ring2] r-aps ring-mac
```

reset erps statistics

Use **reset erps statistics** to clear ERPS packet statistics.

Syntax

reset erps statistics ring *ring-id* [**instance** *instance-id*]

Views

User view

Predefined user roles

network-admin

Parameters

ring *ring-id*: Specifies an ERPS ring by its ID in the range of 1 to 255.

instance *instance-id*: Specifies an ERPS instance by its ID in the range of 1 to 64. If you do not specify this option, this command clears packet statistics for all instances of the ERPS ring.

Examples

Clear packet statistics for instance 1 of ERPS ring 1.

```
<Sysname> reset erps statistics ring 1 instance 1
```

Related commands

display erps statistics

revertive-operation

Use **revertive-operation non-revertive** to set the non-revertive mode for an ERPS ring.

Use **undo revertive-operation** to restore the default.

Syntax

revertive-operation non-revertive

undo revertive-operation

Default

An ERPS ring operates in revertive mode.

Views

ERPS instance view

Predefined user roles

network-admin

Usage guidelines

In non-revertive mode, an owner node does not perform any operations when receiving NR packets. You can use the **erps clear** command to restore the revertive mode.

Examples

Set the non-revertive mode for instance 1 of ERPS ring 1.

```
<Sysname> system-view
[Sysname] erps ring 1
[Sysname-erps-ring1] instance 1
[Sysname-erps-ring1-inst1] revertive-operation non-revertive
```

ring-type sub-ring

Use **ring-type sub-ring** to configure the ERPS ring as a subring.

Use **undo ring-type sub-ring** to restore the default.

Syntax

ring-type sub-ring

undo ring-type

Default

An ERPS ring is a major ring.

Views

ERPS ring view

Predefined user roles

network-admin

Examples

Configure ERPS ring 1 as a subring.

```
<Sysname> system-view
[Sysname] erps ring 1
[Sysname-erps-ring1] ring-type sub-ring
```

sub-ring connect

Use **sub-ring connect** to associate the subring with an ERPS ring.

Use **undo sub-ring connect** to remove the association.

Syntax

sub-ring connect ring *ring-id* **instance** *instance-id*

undo sub-ring connect ring *ring-id* **instance** *instance-id*

Default

A subring is not associated with ERPS rings.

Views

ERPS instance view

Predefined user roles

network-admin

Parameters

ring *ring-id*: Specifies an ERPS ring by its ID in the range of 1 to 255.

instance *instance-id*: Specifies an ERPS instance by its ID in the range of 1 to 64.

Examples

Configure ERPS ring 1 as a subring for instance 1, and associate the subring with ERPS ring 2.

```
<Sysname> system-view
[Sysname] erps ring 2
[Sysname-erps-ring2] instance 1
[Sysname-erps-ring2] quit
[Sysname] erps ring 1
[Sysname-erps-ring1] ring-type sub-ring
[Sysname-erps-ring1] instance 1
[Sysname-erps-ring1-inst1] sub-ring connect ring 2 instance 1
```

Related commands

ring-type sub-ring

timer guard

Use **timer guard** to set the guard timer for an ERPS instance.

Use **undo timer guard** to restore the default.

Syntax

timer guard *guard-value*

undo timer guard

Default

The guard timer is 500 milliseconds for an ERPS instance.

Views

ERPS instance view

Predefined user roles

network-admin

Parameters

guard-value: Specifies the guard timer in the range of 0 to 2000 milliseconds and in step of 10.

Usage guidelines

The guard timer starts when the link recovers. The system processes only the flush packets before the guard timer expires. The guard timer prevents SF messages from impacting the network.

Examples

Set the guard timer to 30 milliseconds for instance 1 of ERPS ring 1.

```
<Sysname> system-view
[Sysname] erps ring 1
[Sysname-erps-ring1] instance 1
[Sysname-erps-ring1-inst1] timer guard 30
```

timer hold-off

Use **timer hold-off** to set the hold-off timer for an ERPS instance.

Use **undo timer hold-off** to restore the default.

Syntax

timer hold-off *hold-off-value*

undo timer hold-off

Default

The hold-off timer is 0 milliseconds for an ERPS instance.

Views

ERPS instance view

Predefined user roles

network-admin

Parameters

hold-off-value: Specifies the hold-off timer in the range of 0 to 10000 milliseconds and in step of 100.

Usage guidelines

The hold-off timer starts when the port detects a link fault. If the link fault persists when the hold-off timer expires, the port reports the link fault. The hold-off timer delays the fault report time and might impact the link recovery performance.

Examples

Set the hold-off timer to 300 milliseconds for instance 1 of ERPS ring 1.

```
<Sysname> system-view
[Sysname] erps ring 1
[Sysname-erps-ring1] instance 1
[Sysname-erps-ring1-inst1] timer hold-off 300
```

timer wtr

Use **timer wtr** to set the WTR timer for an ERPS instance.

Use **undo timer wtr** to restore the default.

Syntax

timer wtr *wtr-value*

undo timer wtr

Default

The WTR timer is 5 minutes for an ERPS instance.

Views

ERPS instance view

Predefined user roles

network-admin

Parameters

wtr-value: Specifies the WTR timer in the range of 1 to 12 minutes and in step of 1.

Usage guidelines

This timer prevents intermittent link failures from impacting the network.

Examples

Set the WTR timer to 3 minutes for instance 1 of ERPS ring 1.

```
<Sysname> system-view
[Sysname] erps ring 1
[Sysname-erps-ring1] instance 1
[Sysname-erps-ring1-inst1] timer wtr 3
```

Contents

Smart Link commands

The following switch series do not support Smart Link:

- S5110V2-SI.
- S5000V3-EI.
- S5000V5-EI.
- S5000E-X.
- S5000X-EI.
- WAS6000.

display smart-link flush

Use **display smart-link flush** to display information about the received flush messages.

Syntax

display smart-link flush

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display information about the received flush messages.

```
<Sysname> display smart-link flush
 Received flush packets                            : 10
 Receiving interface of the last flush packet      : GigabitEthernet1/0/1
 Receiving time of the last flush packet           : 19:19:03 2012/04/21
 Device ID of the last flush packet                : 000f-e200-8500
 Control VLAN of the last flush packet             : 1
```

Table 1 Command output

Field	Description
Received flush packets	Total number of received flush messages.
Receiving interface of the last flush packet	Port that received the last flush message.
Receiving time of the last flush packet	Time when the last flush message was received.
Device ID of the last flush packet	Device ID carried in the last flush message.
Control VLAN of the last flush packet	Control VLAN ID carried in the last flush message.

Related commands

reset smart-link statistics

display smart-link group

Use **display smart-link group** to display information about the specified or all smart link groups.

Syntax

display smart-link group { *group-id* | **all** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group-id: Specifies a smart link group by its ID. The value range for this argument is 1 to 48.

all: Displays information about all smart link groups.

Examples

Display information about smart link group 1.

```
<Sysname> display smart-link group 1
Smart link group 1 information:
  Device ID       : 0011-2200-0001
  Preemption mode : None
  Preemption delay: 1(s)
  Control VLAN    : 1
  Protected VLAN  : Reference Instance 2, 4

  Member                  Role      State   Flush-count     Last-flush-time
  ------------------------------------------------------------------------------
  GE1/0/1                 PRIMARY   ACTIVE  1               16:45:20 2012/04/21
  GE1/0/2                 SECONDARY STANDBY 2               16:37:20 2012/04/21
```

Table 2 Command output

Field	Description
Preemption mode	Preemption mode: • **None**—Preemption disabled. • **Role**—Role preemption mode. • **Speed**—Speed preemption mode.
Preemption delay	Preemption delay time, in seconds.
Control-VLAN	Control VLAN ID.
Protected VLAN	Protected VLANs of the smart link group. Referenced Multiple Spanning Tree Instances (MSTIs) are displayed. To view the VLANs mapped to the referenced MSTIs, use the **display stp region-configuration** command.
Member	Member port of the smart link group.
Role	Port role: primary or secondary.

Field	Description
State	Port state: active, down, or standby.
Flush-count	Number of transmitted flush messages.
Last-flush-time	Time when the last flush message was transmitted (NA indicates that no flush message has been transmitted).

flush enable

Use **flush enable** to enable flush update.

Use **undo flush enable** to disable flush update.

Syntax

flush enable [**control-vlan** *vlan-id*]

undo flush enable

Default

Flush update is enabled for smart link groups, and VLAN 1 is used for flush message transmission.

Views

Smart link group view

Predefined user roles

network-admin

Parameters

control-vlan *vlan-id*: Specifies the control VLAN used for transmitting flush messages. The *vlan-id* argument represents the control VLAN ID and is in the range of 1 to 4094.

Usage guidelines

You must configure different control VLANs for different smart link groups.

- Make sure the configured control VLAN already exists, and assign the smart link group member ports to the control VLAN.
- The control VLAN of a smart link group must also be one of its protected VLANs. Do not remove the control VLAN. Otherwise, flush messages cannot be sent correctly.

Examples

Disable flush update for smart link group 1.

```
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1] undo flush enable
```

Related commands

smart-link flush enable

port

Use **port** to assign a port to a smart link group and specify the port role.

Use **undo port** to remove a port from a smart link group.

Syntax

port *interface-type interface-number* { **primary** | **secondary** }

undo port *interface-type interface-number*

Default

No member ports exist in a smart link group.

Views

Smart link group view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies a port by its type and number, which can be a Layer 2 Ethernet interface or Layer 2 aggregate interface.

primary: Specifies a port as the primary port.

secondary: Specifies a port as the secondary port.

Usage guidelines

Before configuring member ports for a smart link group, you must configure protected VLANs for the smart link group.

Disable the spanning tree feature, RRPP, and ERPS on the ports you want to add to the smart link group. You cannot enable the spanning tree feature, RRPP, or ERPS on a smart link group member port.

If you configure a port as both an aggregation group member and a smart link group member, only the aggregation group member configuration takes effect. The port is not shown in the output from the **display smart-link group** command. The smart link group member configuration takes effect after the port leaves the aggregation group.

You can also assign a port to a smart link group by using the **port smart-link group** command in interface view.

Examples

Configure GigabitEthernet 1/0/1 as the secondary port of smart link group 1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo stp enable
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] smart-link group 1
[Sysname-smlk-group1] protected-vlan reference-instance 0
[Sysname-smlk-group1] port gigabitethernet 1/0/1 secondary
```

Related commands

port smart-link group

port smart-link group

Use **port smart-link group** to assign a port to a smart link group and specify the port role.

Use **undo port smart-link group** to remove a port from a smart link group.

Syntax

port smart-link group *group-id* { **primary** | **secondary** }

undo port smart-link group *group-id*

Default

A port is not a smart link group member.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

group-id: Specifies a smart link group by its ID. The value range for this argument is 1 to 48.

primary: Specifies the port as the primary port.

secondary: Specifies the port as the secondary port.

Usage guidelines

Before configuring member ports for a smart link group, you must configure protected VLANs for the smart link group.

Disable the spanning tree feature, RRPP, and ERPS on the ports you want to add to the smart link group. You cannot enable the spanning tree feature, RRPP, or ERPS on a smart link group member port.

If you configure a port as both an aggregation group member and a smart link group member, only the aggregation group member configuration takes effect. The port is not shown in the output from the **display smart-link group** command. The smart link group member configuration takes effect after the port leaves the aggregation group.

You can assign a port to a smart link group by using the **port** command in smart link group view.

Examples

Configure GigabitEthernet 1/0/1 as the primary port of smart link group 1.

```
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1] protected-vlan reference-instance 0
[Sysname-smlk-group1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo stp enable
[Sysname-GigabitEthernet1/0/1] port smart-link group 1 primary
```

Configure Layer 2 aggregate interface 1 as the primary port of smart link group 1.

```
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1] protected-vlan reference-instance 0
[Sysname-smlk-group1] quit
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] undo stp enable
[Sysname-Bridge-Aggregation1] port smart-link group 1 primary
```

Related commands

port

port smart-link group track

Use **port smart-link group track** to configure the collaboration between a smart link group member port and a track entry.

Use **undo port smart-link group track** to remove the collaboration between a smart link group member port and a track entry.

Syntax

port smart-link group *group-id* **track** *track-entry-number*

undo port smart-link group *group-id* **track** *track-entry-number*

Default

Smart link group member ports do not collaborate with track entries.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

group-id: Specifies a smart link group by its ID. The value range for this argument is 1 to 48.

track-entry-number: Specifies the ID of a track entry that has been associated with the CC function of CFD.

Usage guidelines

Smart Link collaborates with link detection protocols through track entries. It supports only the CC function of CFD to implement link detection. To associate the CC function of CFD with a track entry, use the **track cfd** command.

Before configuring the collaboration between Smart Link and Track on a port, make sure the port has been added to the specified smart link group.

Examples

Configure the collaboration between GigabitEthernet 1/0/1, the primary port of smart link group 1, and the CC function of CFD through track entry 1 to detect the link status.

```
<Sysname> system-view
[Sysname] track 1 cfd cc service-instance 100 mep 2
[Sysname] smart-link group 1
[Sysname-smlk-group1] protected-vlan reference-instance 0
[Sysname-smlk-group1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo stp enable
[Sysname-GigabitEthernet1/0/1] port smart-link group 1 primary
[Sysname-GigabitEthernet1/0/1] port smart-link group 1 track 1
```

Configure the collaboration between bridge-aggregation 1, the primary port of smart link group 1, and the CC function of CFD through track entry 1 to detect the link status.

```
<Sysname> system-view
```

```
[Sysname] track 1 cfd cc service-instance 100 mep 2
[Sysname] smart-link group 1
[Sysname-smlk-group1] protected-vlan reference-instance 0
[Sysname-smlk-group1] quit
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] undo stp enable
[Sysname-Bridge-Aggregation1] port smart-link group 1 primary
[Sysname-Bridge-Aggregation1] port smart-link group 1 track 1
```

Related commands

track cfd

preemption delay

Use **preemption delay** to set the preemption delay.

Use **undo preemption delay** to restore the default.

Syntax

preemption delay *delay*

undo preemption delay

Default

The preemption delay is 1 second.

Views

Smart link group view

Predefined user roles

network-admin

Parameters

delay: Specifies the preemption delay in the range of 0 to 300 seconds.

Usage guidelines

Preemption delay is the period of time that the primary port waits before taking over to collaborate with the switchover of upstream devices.

The preemption delay configuration takes effect only after a preemption mode is configured.

Examples

Enable role preemption and set the preemption delay to 10 seconds.

```
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1] preemption mode role
[Sysname-smlk-group1] preemption delay 10
```

Related commands

preemption mode

preemption mode

Use **preemption mode** to configure a preemption mode for a smart link group.

Use **undo preemption mode** to restore the default.

Syntax

preemption mode { **role** | **speed** [**threshold** *threshold-value*] }

undo preemption mode

Default

No preemption mode is configured for a smart link group.

Views

Smart link group view

Predefined user roles

network-admin

Parameters

role: Specifies the role preemption mode, which enables the primary port to transition to forwarding state after the primary link recovers.

speed: Specifies the speed preemption mode.

threshold *threshold-value*: Specifies the speed preemption threshold in percentage. The value range for the *threshold-value* argument is 1 to 10000.

Usage guidelines

If you specify the speed preemption mode, the following conditions occur when the primary link recovers:

- If you specify the **threshold** *threshold-value* option, the primary port transitions to forwarding state when the following condition is met:

  The difference between the primary port speed and the secondary port speed equals or exceeds the threshold value (in percentage) of the secondary port speed.
- If you do not specify the **threshold** *threshold-value* option, the primary port transitions to forwarding state when the primary port speed exceeds the secondary port speed.

Examples

Configure the role preemption mode.

```
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1] preemption mode role
```

Configure the speed preemption mode and specify the speed preemption threshold as 1000.

```
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1] preemption mode speed threshold 1000
```

protected-vlan

Use **protected-vlan** to configure protected VLANs for a smart link group.

Use **undo protected-vlan** to remove the protected VLAN of a smart link group.

Syntax

protected-vlan reference-instance *instance-id-list*

undo protected-vlan [**reference-instance** *instance-id-list*]

Default

A smart link group does not have protected VLANs.

Views

Smart link group view

Predefined user roles

network-admin

Parameters

reference-instance *instance-id-list*: Specifies protected VLANs.

- When the spanning tree mode is MSTP, the *instance-id-list* argument is a space-separated list of up to 10 MSTI items. Each item specifies an MSTI ID or a range of MSTI IDs in the form of *instance-id 1* **to** *instance-id 2*. The value range for MSTI IDs is 0 to 4094. 0 represents the common internal spanning tree (CIST). The *instance-id 2* must be equal to or greater than *instance-id 1*. You can use the **display stp region-configuration** command to display instance-to-VLAN mappings.
- When the spanning tree mode is PVST, the *instance-id-list* argument is a space-separated list of up to 10 VLAN items. Each item specifies a VLAN ID or a range of VLAN IDs in the form of *instance-id 1* **to** *instance-id 2*. The value range for VLAN IDs is 1 to 4094. The *instance-id 2* must be equal to or greater than *instance-id 1*.

Usage guidelines

You must configure all VLANs to which the member ports of a smart link group belongs as protected VLANs.

If the VLAN-to-MSTI mappings change, the protected VLANs change.

To remove protected VLAN configuration, follow these restrictions and guidelines:

- In MSTP mode, if you specify the **reference-instance** *instance-id-list* option, the **undo protected-vlan** command removes configuration of VLANs mapped to the specified MSTIs. If you do not specify the **reference-instance** *instance-id-list* option, the command removes configuration of all protected VLANs.
- In PVST mode, if you specify the **reference-instance** *instance-id-list* option, the **undo protected-vlan** command removes configuration of the specified VLANs. If you do not specify the **reference-instance** *instance-id-list* option, the command removes configuration of all protected VLANs.
- If a smart link group has member ports, you cannot remove protected VLAN configuration. If a smart link group does not have member ports, you can remove protected VLAN configuration.

Examples

Map VLANs 1 through 30 to MSTI 1, and activate the MST region configuration. Configure the VLANs mapped to MSTI 1 as the protected VLANs of smart link group 1.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] instance 1 vlan 1 to 30
[Sysname-mst-region] active region-configuration
[Sysname-mst-region] quit
[Sysname] smart-link group 1
[Sysname-smlk-group1] protected-vlan reference-instance 1
```

Related commands

display stp region-configuration (*Layer 2—LAN Switching Command Reference*)

smart-link group

reset smart-link statistics

Use **reset smart-link statistics** to clear statistics about flush messages.

Syntax

reset smart-link statistics

Views

User view

Predefined user roles

network-admin

Examples

Clear statistics about flush messages.

```
<Sysname> reset smart-link statistics
```

Related commands

display smart-link flush

smart-link flush enable

Use **smart-link flush enable** to enable flush message receiving.

Use **undo smart-link flush enable** to disable flush message receiving.

Syntax

smart-link flush enable [**control-vlan** *vlan-id-list*]

undo smart-link flush enable [**control-vlan** *vlan-id-list*]

Default

Flush message receiving is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

control-vlan *vlan-id-list*: Specifies a space-separated list of up to 10 control VLAN items. Each item specifies a control VLAN ID or a range of control VLAN IDs in the form of *vlan-id1* **to** *vlan-id2*. The value range for the *vlan-id* argument is 1 to 4094. The *vlan-id2* must be greater than or equal to *vlan-id1*. The default value for the *vlan-id-list* argument is 1.

Examples

Enable GigabitEthernet 1/0/1 to receive flush messages.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] smart-link flush enable
```

Enable Layer 2 aggregate interface 1 to receive flush messages.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] smart-link flush enable
```

Related commands

flush enable

smart-link group

Use **smart-link group** to create a smart link group and enter its view, or enter the view of an existing smart link group.

Use **undo smart-link group** to remove a smart link group.

Syntax

smart-link group *group-id*

undo smart-link group *group-id*

Default

No smart link groups exist.

Views

System view

Predefined user roles

network-admin

Parameters

group-id: Specifies a smart link group ID. The value range for this argument is 1 to 48.

Usage guidelines

You cannot remove a smart link group with member ports.

Examples

Create smart link group 1 and enter its view.

```
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1]
```

Contents

Monitor Link commands

display monitor-link group

Use **display monitor-link group** to display information about monitor link groups.

Syntax

display monitor-link group { *group-id* | **all** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group-id: Specifies a monitor link group by its ID. The value range for the *group-id* argument is 1 to 16.

all: Specifies all monitor link groups.

Usage guidelines

This command does not display information about ports that belong to a link aggregation group.

Examples

Display information about all monitor link groups.

```
<Sysname> display monitor-link group all
Monitor link protocol status: Disabled
Monitor link group 1 information:
  Group status     : N/A
  Downlink up-delay: 0(s)
  Last-up-time     : -
  Last-down-time   : -
  Up-port-threshold: 1

  Member                    Role       Status
  ------------------------------------------------
  GE1/0/1                   UPLINK     UP
  GE1/0/2                   DOWNLINK   UP
```

Table 1 Command output

Field	Description
Monitor link protocol status	Whether Monitor Link is enabled: • Enabled. • Disabled.

Field	Description
Group status	Monitor link group status: • **DOWN**. • **UP**. • **N/A**—Monitor Link is disabled globally. The monitor link group does not operate.
Downlink up-delay	Switchover delay of the downlink interfaces in the monitor link group, in seconds.
Last-up-time	Last time when the monitor link group came up.
Last-down-time	Last time when the monitor link group went down.
Up-port-threshold	Uplink interface threshold for triggering monitor link group state switchover.
Member	Member interfaces of the monitor link group.
Role	Interface role, which can be uplink interface or downlink interface.
Status	Member interface state: • **DOWN**. • **DOWN (Monitor Link)**—The member interface is shut down by Monitor Link. • **UP**.

downlink up-delay

Use **`downlink up-delay`** to set the switchover delay for the downlink interfaces in a monitor link group.

Use **`undo downlink up-delay`** to restore the default.

Syntax

`downlink up-delay` *`delay`*

`undo downlink up-delay`

Default

The switchover delay is 0 seconds. The downlink interfaces come up as soon as an uplink interface in the monitor link group comes up.

Views

Monitor link group view

Predefined user roles

network-admin

Parameters

`delay`: Sets the switchover delay in the range of 1 to 300 seconds.

Usage guidelines

To avoid frequent state changes of downlink interfaces in the event that the uplink interfaces in the monitor link group flap, you can configure a switchover delay. The switchover delay is the time that the downlink interfaces wait before they come up following an uplink interface.

Examples

Set the switchover delay to 50 seconds for the downlink interfaces in monitor link group 1.

```
<Sysname> system-view
[Sysname] monitor-link group 1
[Sysname-mtlk-group1] downlink up-delay 50
```

monitor-link disable

Use **monitor-link disable** to disable Monitor Link globally.

Use **undo monitor-link disable** to enable Monitor Link globally.

Syntax

monitor-link disable

undo monitor-link disable

Default

Monitor Link is enabled globally.

Views

System view

Predefined user roles

network-admin

Usage guidelines

All monitor link groups can operate only after you enable Monitor Link globally. When you disable Monitor Link globally, all monitor link groups cannot operate and the downlink interfaces brought down by the monitor link groups resume their original states.

Examples

Disable Monitor Link globally.

```
<Sysname> system-view
[Sysname] monitor-link disable
```

monitor-link group

Use **monitor-link group** to create a monitor link group and enter its view, or enter the view of an existing monitor link group.

Use **undo monitor-link group** to remove a monitor link group.

Syntax

monitor-link group *group-id*

undo monitor-link group *group-id*

Default

No monitor link groups exist.

Views

System view

Predefined user roles

network-admin

Parameters

group-id: Specifies a monitor link group ID. The value range for the *group-id* argument is 1 to 16.

Examples

Create monitor link group 1 and enter its view.

```
<Sysname> system-view
[Sysname] monitor-link group 1
[Sysname-mtlk-group1]
```

port

Use **port** to assign an interface to a monitor link group.

Use **undo port** to remove an interface from a monitor link group.

Syntax

port *interface-type interface-number* { **downlink** | **uplink** }

undo port *interface-type interface-number*

Default

No member interfaces exist in a monitor link group.

Views

Monitor link group view

Predefined user roles

network-admin

Parameters

interface-type: Specifies an interface by its type.

interface-number: Specifies an interface by its number.

downlink: Specifies a downlink interface.

uplink: Specifies an uplink interface.

Usage guidelines

You can assign an interface to only one monitor link group.

You can also assign an interface to a monitor link group by using the **port monitor-link group** command in interface view.

If you have configured a Selected port of an aggregation group as the downlink interface of a monitor link group, do not configure an Unselected port of the aggregation group as the uplink interface of the monitor link group.

Do not assign an aggregate interface and member ports of the aggregate group to the same monitor link group.

Examples

Configure GigabitEthernet 1/0/1 as an uplink interface and GigabitEthernet 1/0/2 as a downlink interface for monitor link group 1.

```
<Sysname> system-view
[Sysname] monitor-link group 1
[Sysname-mtlk-group1] port gigabitethernet 1/0/1 uplink
```

```
[Sysname-mtlk-group1] port gigabitethernet 1/0/2 downlink
```

Related commands

port monitor-link group

port monitor-link group

Use **port monitor-link group** to assign an interface to a monitor link group.

Use **undo port monitor-link group** to remove an interface from a monitor link group.

Syntax

port monitor-link group *group-id* { **downlink** | **uplink** }

undo port monitor-link group *group-id*

Default

An interface is not a monitor link group member.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Loopback interface view

Predefined user roles

network-admin

Parameters

group-id: Specifies a monitor link group by its ID. The value range for the *group-id* argument is 1 to 16.

downlink: Specifies a downlink interface.

uplink: Specifies an uplink interface.

Usage guidelines

You can assign an interface to only one monitor link group.

You can also assign an interface to a monitor link group by using the **port** command in monitor link group view.

If you have configured a Selected port of an aggregation group as the downlink interface of a monitor link group, do not configure an Unselected port of the aggregation group as the uplink interface of the monitor link group.

Do not assign an aggregate interface and member ports of the aggregate group to the same monitor link group.

Examples

Configure GigabitEthernet 1/0/1 as an uplink interface and GigabitEthernet 1/0/2 as a downlink interface for monitor link group 1.

```
<Sysname> system-view
[Sysname] monitor-link group 1
[Sysname-mtlk-group1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port monitor-link group 1 uplink
[Sysname-GigabitEthernet1/0/1] quit
```

```
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] port monitor-link group 1 downlink
```

Related commands

port

uplink up-port-threshold

Use **uplink up-port-threshold** to configure the uplink interface threshold for triggering monitor link group state switchover.

Use **undo uplink up-port-threshold** to restore the default.

Syntax

uplink up-port-threshold *number-of-port*

undo uplink up-port-threshold

Default

The uplink interface threshold for triggering monitor link group state switchover is 1.

Views

Monitor link group view

Predefined user roles

network-admin

Parameters

number-of-port: Specifies the uplink interface threshold for triggering monitor link group state switchover, in the range of 1 to 1024.

Usage guidelines

When the number of uplink interfaces in up state in a monitor link group is less than the specified threshold, the monitor link group goes down and shuts down its downlink interfaces. When the number of uplink interfaces in up state reaches the threshold, the monitor link group comes up and brings up all its downlink interfaces.

As a best practice, use the **display monitor-link group** command to display the total number of uplink interfaces before executing the **uplink up-port-threshold** command. If you set the threshold to be greater than the total number of uplink interfaces, the monitor link group cannot come up and data will be lost.

Examples

Set the uplink interface threshold for triggering monitor link group state switchover to 5.

```
<Sysname> system-view
[Sysname] monitor-link group 1
[Sysname-mtlk-group1] uplink up-port-threshold 5
```

Contents

VRRP commands

The S5110V2, S5110V2-SI, S5120V3-LI, S5000V3-EI, S5000V5-EI, S5000E-X, S5000X-EI, WS5810-WiNet, and WAS6000 switch series do not support VRRP.

VRRP does not take effect on member ports of aggregation groups.

IPv4 VRRP commands

display vrrp

Use **display vrrp** to display the states of IPv4 VRRP groups.

Syntax

display vrrp [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

vrid *virtual-router-id*: Specifies an IPv4 VRRP group by its virtual router ID. The value range for the *virtual-router-id* argument is 1 to 255.

verbose: Displays detailed IPv4 VRRP group information. If you do not specify the **verbose** keyword, the command displays brief IPv4 VRRP group information.

Usage guidelines

If no interface or VRRP group is specified, this command displays the states of all IPv4 VRRP groups.

If only an interface is specified, this command displays the states of all IPv4 VRRP groups on the specified interface.

If both an interface and an IPv4 VRRP group are specified, this command displays the states of the specified IPv4 VRRP group on the specified interface.

Examples

Display brief information about all IPv4 VRRP groups on the device when VRRP operates in standard mode.

```
<Sysname> display vrrp
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Gratuitous ARP sending interval : 120 sec
 Total number of virtual routers : 1
 Interface          VRID  State        Running Adver   Auth     Virtual
                                        Pri     Timer   Type        IP
```

```
--------------------------------------------------------------------------
Vlan2              1     Master       150     100     Simple   1.1.1.1
```

Table 1 Command output (in standard mode)

Field	Description
Running Mode	VRRP operating mode (standard mode).
Gratuitous ARP sending interval	Sending interval for gratuitous ARP packets. This field is displayed only after you configure the **vrrp send-gratuitous-arp** command.
Total number of virtual routers	Total number of VRRP groups.
Interface	Interface where the VRRP group is configured.
VRID	Virtual router ID (VRRP group number).
State	State of the router in the VRRP group: • **Master**—The router is the master in the VRRP group. • **Backup**—The router is the backup in the VRRP group. • **Initialize**—The router is in **Initialize** state. • **Inactive**—The router is in **Inactive** state, for example, when the router is not assigned a virtual IP address by using the **vrrp vrid** command.
Running Pri	Current priority of the router. When a track entry is associated with a VRRP group on the router, the router's priority changes when the track entry's status changes.
Adver Timer	VRRP advertisement sending interval in centiseconds.
Auth Type	Authentication type: • **None**—No authentication. • **Simple**—Simple text authentication. • **MD5**—MD5 authentication.
Virtual IP	Virtual IP address of the VRRP group.

Display detailed information about all IPv4 VRRP groups on the device when VRRP operates in standard mode.

```
<Sysname> display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Gratuitous ARP sending interval : 120 sec
 Total number of virtual routers : 2
   Interface Vlan-interface2
     VRID             : 1                 Adver Timer  : 100
     Admin Status     : Up                State        : Master
     Config Pri       : 150               Running Pri  : 150
     Preempt Mode     : Yes               Delay Time   : 5
     Auth Type        : Simple            Key          : ******
     Virtual IP       : 1.1.1.1
     Virtual MAC      : 0000-5e00-0101
     Master IP        : 1.1.1.2
     Config Role      : Master
     Name             : abc
   VRRP Track Information:
```

```
  Track Object   : 1                   State : Positive   Pri Reduced : 50

Interface Vlan-interface2
  VRID             : 2                   Adver Timer  : 100
  Admin Status     : Up                  State        : Backup
  Config Pri       : 80                  Running Pri  : 80
  Preempt Mode     : Yes                 Delay Time   : 0
  Become Master    : 2370ms left
  Auth Type        : None
  Virtual IP       : 1.1.1.11
  Virtual MAC      : 0000-5e00-0102
  Master IP        : 1.1.1.12

Interface Vlan-interface2
  VRID             : 3                   Adver Timer : 100
  Admin Status     : Up                  State       : Master
  Config Pri       : 100                 Running Pri : 100
  Preempt Mode     : Yes                 Delay Time  : 0
  Auth Type        : None
  Pkt Sending Mode : v2-only
  Virtual IP       : 1.1.1.10
  Virtual MAC      : 0000-5e00-0103
  Master IP        : 1.1.1.2
  Config Role      : Subordinate
  Follow Name      : abc
```

Table 2 Command output (in standard mode)

Field	Description
Running Mode	VRRP operating mode (standard mode).
Gratuitous ARP sending interval	Sending interval for gratuitous ARP packets. This field is displayed only after you configure the **vrrp send-gratuitous-arp** command.
Total number of virtual routers	Total number of VRRP groups.
Interface	Interface where the VRRP group is configured.
VRID	Virtual router ID (VRRP group number).
Adver Timer	VRRP advertisement sending interval in centiseconds.
Admin Status	Administrative status: **Up** or **Down**.
State	State of the router in the VRRP group: • **Master**—The router is the master in the VRRP group. • **Backup**—The router is the backup in the VRRP group. • **Initialize**—The router is in **Initialize** state. • **Inactive**—The router is in **Inactive** state, for example, when the router is not assigned a virtual IP address by using the **vrrp vrid** command.
Config Pri	Configured priority of the router, which is configured by using the **vrrp vrid priority** command.

Field	Description
Running Pri	Current priority of the router. When a track entry is associated with a VRRP group on the router, the router's priority changes when the track entry's status changes.
Preempt Mode	Preemptive mode: • **Yes**. • **No**.
Delay Time	Preemption delay in centiseconds.
Become Master	Time (in milliseconds) that a backup router has to wait before it becomes the master. This field is displayed only when the router is a backup.
Auth Type	Authentication type: • **None**—No authentication. • **Simple**—Simple text authentication. • **MD5**—MD5 authentication.
Key	Authentication key, which is not displayed if no authentication is required.
Virtual IP	Virtual IP address of the VRRP group.
Virtual MAC	Virtual MAC address of the VRRP group's virtual IP address, which is displayed when the router is the master.
Master IP	Primary IP address of the interface where the master resides.
Config Role	The configured role of the VRRP group to which the router belongs. • **Master**. • **Subordinate**.
Name	Master group name assigned to the VRRP group. This field is displayed only after you configure the **vrrp vrid name** command.
Follow Name	Name of the master VRRP group that the VRRP group follows. This field is displayed only after you configure the **vrrp vrid follow** command.
VRRP Track Information	Track entry information. This field is displayed only after you configure the **vrrp vrid track** command.
Track Object	Track entry which is associated with the VRRP group.
State	Track entry state: • **Negative**. • **Positive**. • **NotReady**.
Pri Reduced	Value by which the priority decreases when the status of the associated track entry changes to the Negative state.
Switchover	Switchover mode. When the status of the associated track entry changes to the Negative state, the backup immediately becomes the master.

Display brief information about all IPv4 VRRP groups on the device when VRRP operates in load balancing mode.

```
<Sysname> display vrrp
IPv4 Virtual Router Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 1
 Interface          VRID  State        Running Address            Active
```

```
                                    Pri
------------------------------------------------------------------------
Vlan2               1     Master       150     1.1.1.1             Local
-----               VF1   Active       255     000f-e2ff-0011      Local
```

Table 3 Command output (in load balancing mode)

Field	Description
Running Mode	VRRP operating mode (load balancing mode).
Total number of virtual routers	Total number of VRRP groups.
Interface	Interface where the VRRP group is configured.
VRID	Virtual router ID (VRRP group number) or virtual forwarder (VF) ID.

State	• For a VRRP group, this field indicates the state of the router in the VRRP group:
	  ◦ **Master**—The router is the master in the VRRP group.
	  ◦ **Backup**—The router is the backup in the VRRP group.
	  ◦ **Initialize**—The router is in **Initialize** state.
	  ◦ **Inactive**—The router is in **Inactive** state, for example, when the router is not assigned a virtual IP address by using the **vrrp vrid** command.
	• For a VF, this field indicates the state of the VF in the VRRP group:
	  ◦ **Active**—The VF is created on the device.
	  ◦ **Listening**—The VF is learned from another device.
	  ◦ **Initialize**—The VF is in **Initialize** state.

Running Pri	• For a VRRP group, this field indicates the running priority of the router. When a track entry is associated with a VRRP group on the router, the router's priority changes when the track entry's status changes. • For a VF, this field indicates the running priority of the VF. When a track entry is associated with a VF, the priority of the VF changes if the track entry's status changes.
Address	• For a VRRP group, this field indicates the virtual IP address of the VRRP group. • For a VF, this field indicates the virtual MAC address of the VF.
Active	• For a VRRP group, this field indicates the IP address of the interface where the master resides. If the current router is the master, this field displays **local**. • For a VF, this field indicates the IP address of the interface where the active virtual forwarder (AVF) resides. If the current VF is the AVF, this field displays **local**.

Display detailed information about all IPv4 VRRP groups on the device when VRRP operates in load balancing mode.

```
<Sysname> display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 2
   Interface Vlan-interface2
     VRID           : 1                 Adver Timer  : 100
     Admin Status   : Up                State        : Master
     Config Pri     : 150               Running Pri  : 150
     Preempt Mode   : Yes               Delay Time   : 5
```

```
  Auth Type      : None
  Virtual IP     : 10.1.1.1
                   10.1.1.2
                   10.1.1.3
  Member IP List : 10.1.1.10 (Local, Master)
                   10.1.1.20 (Backup)
VRRP Track Information:
  Track Object   : 1                    State : Positive   Pri Reduced : 50
Forwarder Information: 2 Forwarders 1 Active
  Config Weight  : 255
  Running Weight : 255
 Forwarder 01
  State          : Active
  Virtual MAC    : 000f-e2ff-0011 (Owner)
  Owner ID       : 0000-5e01-1101
  Priority       : 255
  Active         : local
 Forwarder 02
  State          : Listening
  Virtual MAC    : 000f-e2ff-0012 (Learnt)
  Owner ID       : 0000-5e01-1103
  Priority       : 127
  Active         : 10.1.1.20
Forwarder Weight Track Information:
  Track Object   : 1          State : Positive   Weight Reduced : 250
Interface Vlan-interface2
  VRID           : 11                   Adver Timer  : 100
  Admin Status   : Up                   State        : Backup
  Config Pri     : 80                   Running Pri  : 80
  Preempt Mode   : Yes                  Delay Time   : 0
  Become Master  : 2370ms left
  Auth Type      : None
  Virtual IP     : 10.1.1.11
                   : 10.1.1.12
                   : 10.1.1.13
  Member IP List : 10.1.1.10 (Local, Backup)
                   10.1.1.15 (Master)
Forwarder Information: 2 Forwarders 1 Active
  Config Weight  : 255
  Running Weight : 255
 Forwarder 01
  State          : Active
  Virtual MAC    : 000f-e2ff-40b1 (Learnt)
  Owner ID       : 0000-5e01-1103
  Priority       : 127
  Active         : 10.1.1.15
 Forwarder 02
  State          : Listening
```

```
Virtual MAC    : 000f-e2ff-40b2 (Owner)
Owner ID       : 0000-5e01-1101
Priority       : 255
Active         : local
```

Table 4 Command output (in load balancing mode)

Field	Description
Running Mode	VRRP operating mode (load balancing mode).
Total number of virtual routers	Total number of VRRP groups.
Interface	Interface where the VRRP group is configured.
VRID	Virtual router ID (VRRP group number).
Adver Timer	VRRP advertisement sending interval in centiseconds.
Admin Status	Administrative status: **Up** or **Down**.
State	State of the router in the VRRP group: • **Master**—The router is the master in the VRRP group. • **Backup**—The router is the backup in the VRRP group. • **Initialize**—The router is in **Initialize** state. • **Inactive**—The router is in **Inactive** state, for example, when the router is not assigned a virtual IP address by using the **vrrp vrid** command.
Config Pri	Configured priority of the router, which is configured by using the **vrrp vrid priority** command.
Running Pri	Current priority of the router. When a track entry is associated with a VRRP group on the router, the router's priority changes when the track entry's status changes.
Preempt Mode	Preemptive mode: • **Yes**. • **No**.
Delay Time	Preemption delay in centiseconds.
Become Master	Time (in milliseconds) that a backup router has to wait before it becomes the master. This field is displayed only when the router is a backup.
Auth Type	Authentication type: • **None**—No authentication. • **Simple**—Simple text authentication. • **MD5**—MD5 authentication.
Key	Authentication key, which is not displayed if no authentication is required.
Virtual IP	Virtual IP address list of the VRRP group.
Member IP List	IP addresses of the member devices in the VRRP group: • **Local**—IP address of the local router. • **Master**—IP address of the master. • **Backup**—IP address of the backup.
VRRP Track Information	Track entry which is associated with the VRRP group. This field is displayed only after you configure the **vrrp vrid track** command.
Track Object	Track entry to be monitored.

Field	Description
State	Track entry state: • **Negative**. • **Positive**. • **NotReady**.
Pri Reduced	Value by which the priority decreases when the status of the associated track entry changes to the Negative state. This field is displayed only after you configure the **vrrp vrid track** command.
Switchover	Switchover mode. When the status of the associated track entry changes to the Negative state, the backup immediately becomes the master.
Forwarder Information: 2 Forwarders 1 Active	VF information: Two VFs exist, and one is the AVF.
Config Weight	Configured weight of the VF: 255.
Running Weight	Current weight of the VF. When a track entry is associated with the VFs of a VRRP group, the VFs' weights change when the track entry's status changes.
Forwarder 01	Information about VF 01.
State	VF state: • **Active**—The VF is created on the device. • **Listening**—The VF is learned from another device. • **Initialize**—The VF is in **Initialize** state.
Virtual MAC	Virtual MAC address of the VF.
Owner ID	Real MAC address of the VF owner.
Priority	VF priority in the range of 1 to 255.
Active	IP address of the interface where the AVF resides. If the current VF is the AVF, this field displays **local**.
Forwarder Weight Track Configuration	VF weight Track configuration. The field is displayed only after you configure the **vrrp vrid track** command.
Track Object	Track entry that is associated with the VFs. The field is displayed only after you configure the **vrrp vrid track** command.
State	Track entry state: • **Negative**. • **Positive**. • **NotReady**.
Weight Reduced	Value by which the weights of the VFs decrease when the state of the associated track entry changes to Negative. The field is displayed only after you configure the **vrrp vrid track** command.
Forwarder Switchover Track Information:	VF switchover Track configuration. The field is displayed only after you configure the **vrrp vrid track** command.
Member IP	IP address of a member device. The field is displayed only after you configure the **vrrp vrid track** command.

display vrrp binding

Use **display vrrp binding** to display master-to-subordinate IPv4 VRRP group bindings.

Syntax

display vrrp binding [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*] | **name** *name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. The interface must be an interface to which master IPv4 VRRP groups belong.

vrid *virtual-router-id*: Specifies a master IPv4 VRRP group by its virtual router ID. The value range for the *virtual-router-id* argument is 1 to 255.

name *name*: Specifies a master IPv4 VRRP group by its name, a case-sensitive string of 1 to 20 characters.

Usage guidelines

If you do not specify any parameters, this command displays all master-to-subordinate IPv4 VRRP group bindings.

If you specify an interface but do not specify the virtual router ID of a master VRRP group, this command displays all master-to-subordinate VRRP group bindings on the specified interface.

If you specify an interface and the virtual router ID of a master VRRP group, this command displays the binding information about the specified master VRRP group on the specified interface.

Examples

Display master-to-subordinate IPv4 VRRP group bindings.

```
<Sysname> display vrrp binding
IPv4 virtual router binding information:
  Total number of master virtual routers           : 1
  Total number of subordinate virtual routers      : 2
  Interface : Vlan2                    Master VRID : 1
  Name      : a                        Status      : Backup
  Subordinate virtual routers : 1
    Interface : Vlan2                  VRID        : 4

  Interface : --                       Master VRID : --
  Name      : c                        Status      : --
  Subordinate virtual routers : 1
    Interface : Vlan2                  VRID        : 5
```

Table 5 Command output

Field	Description
Total number of master virtual routers	Total number of master VRRP groups.
Total number of subordinate virtual routers	Total number of subordinate VRRP groups.
Interface	Interface to which the master VRRP group belongs. If the master VRRP group does not exist, this field displays two hyphens (**--**).
Master VRID	Virtual router ID of the master VRRP group. If the master VRRP group does not exist, this field displays two hyphens (**--**).
Name	Name of the master VRRP group.
Status	Status of the router in the master VRRP group: • **Master**. • **Backup**. • **Initialize**. • **Inactive**. If the master VRRP group does not exist, this field displays two hyphens (**--**).
Subordinate virtual routers	Number of subordinate VRRP groups.
Interface	Interface to which the subordinate VRRP group belongs.
VRID	Virtual router ID of the subordinate VRRP group.

Related commands

`vrrp vrid follow`

`vrrp vrid name`

display vrrp statistics

Use **`display vrrp statistics`** to display statistics for IPv4 VRRP groups.

Syntax

`display vrrp statistics` [**`interface`** *`interface-type interface-number`* [**`vrid`** *`virtual-router-id`*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

`interface` *`interface-type interface-number`*: Specifies an interface by its type and number.

`vrid` *`virtual-router-id`*: Specifies an IPv4 VRRP group by its virtual router ID. The value range for the *`virtual-router-id`* argument is 1 to 255.

Usage guidelines

If no interface or VRRP group is specified, this command displays statistics for all IPv4 VRRP groups.

If only an interface is specified, this command displays statistics for all IPv4 VRRP groups on the specified interface.

If both an interface and an IPv4 VRRP group are specified, this command displays statistics for the specified IPv4 VRRP group on the specified interface.

Examples

Display statistics for all IPv4 VRRP groups when VRRP operates in standard mode.

```
<Sysname> display vrrp statistics
 Interface              : Vlan-interface2
 VRID                   : 1
 CheckSum Errors        : 0          Version Errors               : 0
 Invalid Pkts Rcvd  :     0          Unexpected Pkts Rcvd         : 0
 IP TTL Errors          : 0          Advertisement Interval Errors : 0
 Invalid Auth Type      : 0          Auth Failures                : 0
 Packet Length Errors   : 0          Auth Type Mismatch           : 0
 Become Master          : 1          Address List Errors          : 0
 Adver Rcvd             : 0          Priority Zero Pkts Rcvd      : 0
 Adver Sent             : 807        Priority Zero Pkts Sent      : 0
IP Owner Conflicts     : 0

 Global statistics
 CheckSum Errors        : 0
 Version Errors         : 0
 VRID Errors            : 0
```

Display statistics for all IPv4 VRRP groups when VRRP operates in load balancing mode.

```
<Sysname> display vrrp statistics
 Interface              : Vlan-interface2
 VRID                   : 1
 CheckSum Errors        : 0          Version Errors               : 0
 Invalid Pkts Rcvd      : 0          Unexpected Pkts Rcvd         : 0
 IP TTL Errors          : 0          Advertisement Interval Errors : 0
 Invalid Auth Type      : 0          Auth Failures                : 0
 Packet Length Errors   : 0          Auth Type Mismatch           : 0
 Become Master          : 39         Address List Errors          : 0
 Become AVF             : 13         Packet Option Errors         : 0
 Adver Rcvd             : 2562       Priority Zero Pkts Rcvd      : 1
 Adver Sent             : 16373      Priority Zero Pkts Sent      : 49
 Request Rcvd           : 2          Reply Rcvd                   : 10
 Request Sent           : 12         Reply Sent                   : 2
 Release Rcvd           : 0          VF Priority Zero Pkts Rcvd   : 1
 Release Sent           : 0          VF Priority Zero Pkts Sent   : 11
 Redirect Timer Expires  : 1         Time-out Timer Expires       : 0

 Global statistics
 CheckSum Errors        : 0
```

```
Version Errors          : 0
VRID Errors             : 0
```

Table 6 Command output (in standard mode)

Field	Description
Interface	Interface where the VRRP group is configured.
VRID	VRRP group number.
CheckSum Errors	Number of packets with checksum errors.
Version Errors	Number of packets with version errors.
Invalid Pkts Rcvd	Number of received packets of invalid packet types.
Unexpected Pkts Rcvd	Number of received unexpected packets.
Advertisement Interval Errors	Number of packets with advertisement interval errors.
IP TTL Errors	Number of packets with TTL errors.
Auth Failures	Number of packets with authentication failures.
Invalid Auth Type	Number of packets with authentication failures because of invalid authentication types.
Auth Type Mismatch	Number of packets with authentication failures because of mismatching authentication types.
Packet Length Errors	Number of packets with VRRP packet length errors.
Address List Errors	Number of packets with virtual IP address list errors.
Become Master	Number of times that the router has been elected as the master.
Priority Zero Pkts Rcvd	Number of received advertisements with the router priority of 0.
Adver Rcvd	Number of received advertisements.
Priority Zero Pkts Sent	Number of sent advertisements with the router priority of 0.
Adver Sent	Number of sent advertisements.
IP Owner Conflicts	Number of VRRP packets that the local router (IP address owner) has received from conflicting IP address owners.
Global statistics	Global statistics for all VRRP groups.
CheckSum Errors	Total number of packets with checksum errors.
Version Errors	Total number of packets with version errors.
VRID Errors	Total number of packets with VRID errors.

Table 7 Command output (in load balancing mode)

Field	Description
Interface	Interface where the VRRP group is configured.
VRID	VRRP group number.
CheckSum Errors	Number of packets with checksum errors.
Version Errors	Number of packets with version errors.
Invalid Pkts Rcvd	Number of received packets of invalid packet types.

Field	Description
Unexpected Pkts Rcvd	Number of received unexpected packets.
Advertisement Interval Errors	Number of packets with advertisement interval errors.
IP TTL Errors	Number of packets with TTL errors.
Auth Failures	Number of packets with authentication failures.
Invalid Auth Type	Number of packets with authentication failures because of invalid authentication types.
Auth Type Mismatch	Number of packets with authentication failures because of mismatching authentication types.
Packet Length Errors	Number of packets with VRRP packet length errors.
Address List Errors	Number of packets with virtual IP address list errors.
Become Master	Number of times that the router has been elected as the master.
Redirect Timer Expires	Number of times that the redirect timer expired.
Become AVF	Number of times that the VF has been elected as the AVF.
Time-out Timer Expires	Number of times that the time-out timer expired.
Adver Rcvd	Number of received advertisements.
Request Rcvd	Number of received requests.
Adver Sent	Number of sent advertisements.
Request Sent	Number of sent requests.
Reply Rcvd	Number of received replies.
Release Rcvd	Number of received release packets.
Reply Sent	Number of sent replies.
Release Sent	Number of sent release packets.
Priority Zero Pkts Rcvd	Number of received advertisements with the router priority of 0.
VF Priority Zero Pkts Rcvd	Number of received advertisements with the VF priority of 0.
Priority Zero Pkts Sent	Number of sent advertisements with the router priority of 0.
VF Priority Zero Pkts Sent	Number of sent advertisements with the VF priority of 0.
Packet Option Errors	Number of packet option errors.
Global statistics	Global statistics for all IPv4 VRRP groups.
CheckSum Errors	Total number of packets with checksum errors.
Version Errors	Total number of packets with version errors.
VRID Errors	Total number of packets with VRID errors.

Related commands

`reset vrrp statistics`

reset vrrp statistics

Use **`reset vrrp statistics`** to clear statistics for IPv4 VRRP groups.

Syntax

reset vrrp statistics [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

vrid *virtual-router-id*: Specifies an IPv4 VRRP group by its virtual router ID. The value range for the *virtual-router-id* argument is 1 to 255.

Usage guidelines

If no interface or VRRP group is specified, this command clears statistics for all IPv4 VRRP groups.

If only an interface is specified, this command clears statistics for all IPv4 VRRP groups on the specified interface.

If both an interface and an IPv4 VRRP group are specified, this command clears statistics for the specified IPv4 VRRP group on the specified interface.

Examples

Clear statistics for all IPv4 VRRP groups on all interfaces.

```
<Sysname> reset vrrp statistics
```

Related commands

display vrrp statistics

snmp-agent trap enable vrrp

Use **snmp-agent trap enable vrrp** to enable SNMP notifications for VRRP.

Use **undo snmp-agent trap enable vrrp** to disable SNMP notifications for VRRP.

Syntax

snmp-agent trap enable vrrp [**auth-failure** | **new-master**]

undo snmp-agent trap enable vrrp [**auth-failure** | **new-master**]

Default

SNMP notifications for VRRP are enabled.

Views

System view

Predefined user roles

network-admin

Parameters

auth-failure: Generates notifications as defined in RFC 2787 when the device in a VRRP group receives a VRRP advertisement with the authentication type or key not matching the local configuration.

new-master: Generates notifications as defined in RFC 2787 when the state of a device in a VRRP group changes from Initialize or Backup to Master.

Usage guidelines

To report critical VRRP events to an NMS, enable SNMP notifications for VRRP. For VRRP event notifications to be sent correctly, you must also configure SNMP on the device. For more information about SNMP configuration, see the network management and monitoring configuration guide for the device.

Examples

Generate notifications as defined in RFC 2787 when the device in a VRRP group receives a VRRP advertisement with the authentication type or key not matching the local configuration.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable vrrp auth-failure
```

vrrp check-ttl enable

Use **vrrp check-ttl enable** to enable TTL check for IPv4 VRRP packets.

Use **undo vrrp check-ttl enable** to disable TTL check for IPv4 VRRP packets.

Syntax

vrrp check-ttl enable

undo vrrp check-ttl enable

Default

TTL check for IPv4 VRRP packets is enabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

The master in an IPv4 VRRP group periodically sends VRRP advertisements to declare its presence. The VRRP advertisements are multicast in the local subnet and cannot be forwarded by routers, so the TTL value is not changed. When the master sends VRRP advertisements, it sets the TTL value to 255. If you enable TTL check, the backups drop the VRRP advertisements with TTL other than 255, preventing attacks from other subnets.

Devices from different vendors might implement VRRP differently. When the device is interoperating with devices of other vendors, TTL check on VRRP packets might result in unexpected dropping of packets. In this scenario, use the **undo vrrp check-ttl enable** command to disable TTL check on VRRP packets.

Examples

Disable TTL check for IPv4 VRRP packets.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] undo vrrp check-ttl enable
```

vrrp dscp

Use **vrrp dscp** to set a DSCP value for VRRP packets.

Use **undo vrrp dscp** to restore the default.

Syntax

vrrp dscp *dscp-value*

undo vrrp dscp

Default

The DSCP value for VRRP packets is 48.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies a DSCP value for VRRP packets, in the range of 0 to 63.

Usage guidelines

The DSCP value identifies the packet priority during transmission. A greater DSCP value means a higher packet priority.

Examples

Set the DSCP value to 30 for VRRP packets.

```
<Sysname> system-view
[Sysname] vrrp dscp 30
```

vrrp mode

Use **vrrp mode** to specify the operating mode for IPv4 VRRP.

Use **undo vrrp mode** to restore the default.

Syntax

vrrp mode load-balance [**version-8**]

undo vrrp mode

Default

IPv4 VRRP operates in standard mode.

Views

System view

Predefined user roles

network-admin

Parameters

load-balance: Specifies the load balancing mode.

version-8: Specifies the version carried in VRRP packets as 8.

Usage guidelines

After you create IPv4 VRRP groups on the router, you can use this command to modify their operating mode. All IPv4 VRRP groups on the router operate in the specified mode.

The **version-8** keyword takes effect only when the version of IPv4 VRRP configured on the interface is VRRPv2. The **version-8** keyword is required in the following conditions:

- A router running Comware 5 software exists in the VRRP group.

  To display the software version, use the **display version** command.
- All routers in the IPv4 VRRP group are operating in load balancing mode.
- All routers in the IPv4 VRRP group are configured with the version of VRRPv2.

Examples

Specify the load balancing mode for IPv4 VRRP.

```
<Sysname> system-view
[Sysname] vrrp mode load-balance
```

Related commands

display vrrp

vrrp send-gratuitous-arp

Use **vrrp send-gratuitous-arp** to enable periodic sending of gratuitous ARP packets for IPv4 VRRP.

Use **undo vrrp send-gratuitous-arp** to disable periodic sending of gratuitous ARP packets for IPv4 VRRP.

Syntax

vrrp send-gratuitous-arp [**interval** *interval*]

undo vrrp send-gratuitous-arp

Default

Periodic sending of gratuitous ARP packets is disabled for IPv4 VRRP.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the sending interval in the range of 30 to 1200 seconds. The default value is 120 seconds.

Usage guidelines

This command ensures that the MAC address entry for the virtual MAC address of a VRRP group can be updated on downstream devices in a timely manner.

This command takes effect only in VRRP standard mode.

If you change the sending interval for gratuitous ARP packets, the configuration takes effect at the next sending interval.

The master sends the first gratuitous ARP packet at a random time in the second half of the set interval after you execute the **vrrp send-gratuitous-arp** command. This prevents too many gratuitous ARP packets from being sent at the same time.

The sending interval for gratuitous ARP packets might be much longer than the set interval when the following conditions are met:

- Multiple VRRP groups exist on the device.

- A short sending interval is set.

Examples

Enable periodic sending of gratuitous ARP packets for IPv4 VRRP and set the sending interval to 200 seconds.

```
<Sysname> system-view
[Sysname] vrrp send-gratuitous-arp interval 200
```

vrrp version

Use **vrrp version** to specify the version of IPv4 VRRP on an interface.

Use **undo vrrp version** to restore the default.

Syntax

vrrp version *version-number*

undo vrrp version

Default

VRRPv3 is used.

Views

Interface view

Predefined user roles

network-admin

Parameters

version-number: Specifies a VRRP version. The version number is 2 or 3, where 2 indicates VRRPv2 (described in RFC 3768), and 3 indicates VRRPv3 (described in RFC 5798).

Usage guidelines

The version of VRRP on all routers in an IPv4 VRRP group must be the same.

Examples

Specify VRRPv2 to run on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] vrrp version 2
```

vrrp vrid

Use **vrrp vrid** to create an IPv4 VRRP group and assign a virtual IP address to it, or to assign a virtual IP address to an existing IPv4 VRRP group.

Use **undo vrrp vrid** to remove all configurations of an IPv4 VRRP group, or to remove a virtual IP address from an IPv4 VRRP group.

Syntax

vrrp vrid *virtual-router-id* **virtual-ip** *virtual-address*

undo vrrp vrid *virtual-router-id* [**virtual-ip** [*virtual-address*]]

Default

No IPv4 VRRP groups exist.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID. The value range for the *virtual-router-id* argument is 1 to 255.

virtual-ip *virtual-address*: Specifies a virtual IP address. You cannot specify the virtual IP address as any of the following IP addresses:

- All-zero address (0.0.0.0).
- Broadcast address (255.255.255.255).
- Loopback address.
- IP address of other than Class A, Class B, and Class C.
- Invalid IP address (for example, 0.0.0.1).

If you do not specify the *virtual-address* argument, the **undo vrrp vrid** command removes all virtual IP addresses from the specified IPv4 VRRP group.

Usage guidelines

You can execute this command multiple times to assign multiple virtual IP addresses to an IPv4 VRRP group. An IPv4 VRRP group can have a maximum of 16 virtual IP addresses.

An IPv4 VRRP group without virtual IP addresses configured can exist on a device provided that other settings (for example, priority and preemption mode) are available. Such a VRRP group stays in inactive state and does not function.

The virtual IP address of an IPv4 VRRP group and the downlink interface IP addresses of the VRRP group members must be in the same subnet. Otherwise, the hosts in the subnet might fail to access external networks.

For VRRP to operate correctly in load balancing mode, make sure the virtual IP address of an IPv4 VRRP group is not the IP address of any interfaces in the VRRP group.

Examples

Create IPv4 VRRP group 1 and assign virtual IP address 10.10.10.10 to the VRRP group. Then assign virtual IP address 10.10.10.11 to the VRRP group.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.10.10.10
[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.10.10.11
```

Related commands

display vrrp

vrrp vrid authentication-mode

Use **vrrp vrid authentication-mode** to configure the authentication mode and the authentication key for an IPv4 VRRP group to send and receive VRRP packets.

Use **undo vrrp vrid authentication-mode** to restore the default.

Syntax

vrrp vrid *virtual-router-id* **authentication-mode** { **md5** | **simple** } { **cipher** | **plain** } *string*

undo vrrp vrid *virtual-router-id* **authentication-mode**

Default

Authentication is disabled when a VRRP group sends and receives VRRP packets.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID. The value range for the *virtual-router-id* argument is 1 to 255.

md5: Specifies the MD5 authentication mode.

simple: Specifies the simple authentication mode.

cipher: Specifies a key in encrypted form.

plain: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. Its plaintext form is a case-sensitive string of 1 to 8 characters. Its encrypted form is a case-sensitive string of 1 to 41 characters.

Usage guidelines

To avoid attacks from unauthorized users, VRRP member routers add authentication keys in VRRP packets to authenticate one another. VRRP provides the following authentication modes:

- **simple**—Simple text authentication.

  The sender fills an authentication key into the VRRP packet, and the receiver compares the received authentication key with its local authentication key. If the two authentication keys are the same, the received VRRP packet is legitimate. Otherwise, the received packet is illegitimate.

- **md5**—MD5 authentication.

  The sender computes a digest for the VRRP packet by using the authentication key and MD5 algorithm, and saves the result to the authentication header. The receiver performs the same operation by using the authentication key and MD5 algorithm, and it compares the result with the content in the authentication header. If the results are the same, the received VRRP packet is legitimate. Otherwise, the received packet is illegitimate.

The MD5 authentication is more secure than the simple text authentication, but it costs more resources.

IMPORTANT:

- You can configure different authentication modes and authentication keys for the VRRP groups on an interface. However, members of the same VRRP group must use the same authentication mode and authentication key.
- For VRRPv3, this command does not take effect because VRRPv3 does not support authentication.

Examples

Set the authentication mode to **simple** and the authentication key to **Sysname** for VRRP group 1 on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 authentication-mode simple plain Sysname
```

Related commands

display vrrp

vrrp version

vrrp vrid follow

Use **vrrp vrid follow** to configure an IPv4 VRRP group to follow a master group.

Use **undo vrrp vrid follow** to remove the configuration.

Syntax

vrrp vrid *virtual-router-id* **follow** *name*

undo vrrp vrid *virtual-router-id* **follow**

Default

An IPv4 VRRP group does not follow a master group.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID. The value range for the *virtual-router-id* argument is 1 to 255.

name: Specifies a master IPv4 VRRP group by its name, a case-sensitive string of 1 to 20 characters.

Usage guidelines

This command configures an IPv4 VRRP group as a subordinate VRRP group to follow a master group. A subordinate VRRP group can forward service traffic.

An IPv4 VRRP group cannot be both a master group and a subordinate group.

An IPv4 VRRP group stays in **Inactive** state if it is configured to follow a nonexistent master VRRP group.

If an IPv4 VRRP group in **Inactive** or **Initialize** state follows a master group that is not in **Inactive** state, the state of the VRRP group does not change.

Examples

Configure IPv4 VRRP group 1 to follow master group **abc**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 follow abc
```

Related commands

display vrrp binding

vrrp vrid name

vrrp vrid name

Use **vrrp vrid name** to configure an IPv4 VRRP group as a master group and assign a name to it.

Use **undo vrrp vrid name** to remove the configuration.

Syntax

vrrp vrid *virtual-router-id* **name** *name*

undo vrrp vrid *virtual-router-id* **name**

Default

An IPv4 VRRP group does not act as a master group.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID. The value range for the *virtual-router-id* argument is 1 to 255.

name: Specifies a master IPv4 VRRP group name, a case-sensitive string of 1 to 20 characters.

Usage guidelines

This command configures an IPv4 VRRP group as a master group by assigning a master group name to it. A VRRP group that follows the master group is a subordinate VRRP group. The master VRRP group exchanges VRRP packets among member devices. The subordinate VRRP group does not exchange VRRP packets and follows the state of the master group. Both the master and subordinate VRRP groups can forward service traffic.

You cannot assign the same master VRRP group name to different VRRP groups on a device.

Examples

Configure IPv4 VRRP group 1 as a master group and assign master group name **abc** to it.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 name abc
```

Related commands

display vrrp binding

vrrp vrid follow

vrrp vrid preempt-mode

Use **vrrp vrid preempt-mode** to enable the preemptive mode for the device in an IPv4 VRRP group and set the preemption delay.

Use **undo vrrp vrid preempt-mode** to disable the preemptive mode for the device in an IPv4 VRRP group.

Use **undo vrrp vrid preempt-mode delay** to restore the default preemption delay.

Syntax

vrrp vrid *virtual-router-id* **preempt-mode** [**delay** *delay-value*]

undo vrrp vrid *virtual-router-id* **preempt-mode** [**delay**]

Default

The device operates in preemptive mode and the preemption delay is 0 centiseconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID. The value range for the *virtual-router-id* argument is 1 to 255.

delay *delay-value*: Specifies the preemption delay in the range of 0 to 180000 in centiseconds.

Usage guidelines

In non-preemptive mode, the master router acts as the master as long as it operates correctly, even if a backup is assigned a higher priority later. The non-preemptive mode helps avoid frequent switchover between the master and backups.

In preemptive mode, a backup sends VRRP advertisements when it detects that it has a higher priority than the master. Then the backup takes over as the master and the previous master becomes a backup. This mechanism ensures that the master is always the device with the highest priority.

You can configure the VRRP preemption delay for the following purposes:

- Avoid frequent state changes among members in a VRRP group.
- Provide the backups with enough time to collect information (such as routing information).

A backup does not immediately become the master after it receives an advertisement with a lower priority than the local priority. Instead, it waits for a period of time before taking over as the master.

Examples

Enable the preemptive mode for the device in VRRP group 1, and set the preemption delay to 5000 centiseconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 preempt-mode delay 5000
```

Related commands

display vrrp

vrrp vrid priority

Use **vrrp vrid priority** to set the priority of the device in an IPv4 VRRP group.

Use **undo vrrp vrid priority** to restore the default.

Syntax

vrrp vrid *virtual-router-id* **priority** *priority-value*

undo vrrp vrid *virtual-router-id* **priority**

Default

The priority of a device in an IPv4 VRRP group is 100.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID. The value range for the *virtual-router-id* argument is 1 to 255.

priority-value: Specifies a priority value in the range of 1 to 254. A higher value indicates a higher priority.

Usage guidelines

VRRP determines the role (master or backup) of each device in a VRRP group by priority. A device with a higher priority is more likely to become the master.

Priorities 1 to 254 are configurable. Priority 0 is reserved for special uses, and priority 255 is for the IP address owner. The IP address owner in a VRRP group always has a running priority of 255 and acts as the master as long as it operates correctly.

Examples

Set the priority of the switch to 150 in VRRP group 1 on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 priority 150
```

Related commands

display vrrp

vrrp vrid track

vrrp vrid shutdown

Use **vrrp vrid shutdown** to disable an IPv4 VRRP group.

Use **undo vrrp vrid shutdown** to enable an IPv4 VRRP group.

Syntax

vrrp vrid *virtual-router-id* **shutdown**

undo vrrp vrid *virtual-router-id* **shutdown**

Default

An IPv4 VRRP group is enabled.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID. The value range for the *virtual-router-id* argument is 1 to 255.

Usage guidelines

You can use this command to temporarily disable an IPv4 VRRP group. After this command is configured, the VRRP group stays in **Initialize** state, and its configurations remain unchanged. You can change the configuration of the VRRP group, and your changes take effect when you enable the VRRP group again.

Examples

Disable IPv4 VRRP group 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 shutdown
```

vrrp vrid source-interface

Use **vrrp vrid source-interface** to specify the source interface for an IPv4 VRRP group, instead of the interface where the VRRP group resides, to send and receive VRRP packets.

Use **undo vrrp source-interface** to cancel the specified source interface.

Syntax

vrrp vrid *virtual-router-id* **source-interface** *interface-type interface-number*

undo vrrp vrid *virtual-router-id* **source-interface**

Default

No source interface is specified for a VRRP group. The interface where the VRRP group resides sends and receives VRRP packets.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID. The value range for the *virtual-router-id* argument is 1 to 255.

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

If VRRP group members cannot exchange VRRP packets through the interfaces where the VRRP group resides, use this command to specify interfaces for VRRP packet exchange.

Examples

Specify VLAN-interface 20 as the source interface for VRRP packet exchange in IPv4 VRRP group 10.

```
<Sysname> system-view
```

```
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] vrrp vrid 10 source-interface vlan-interface 20
```

vrrp vrid timer advertise

Use **vrrp vrid timer advertise** to set the interval at which the master in an IPv4 VRRP group sends VRRP advertisements.

Use **undo vrrp vrid timer advertise** to restore the default.

Syntax

vrrp vrid *virtual-router-id* **timer advertise** *adver-interval*

undo vrrp vrid *virtual-router-id* **timer advertise**

Default

The master in an IPv4 VRRP group sends VRRP advertisements at an interval of 100 centiseconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID. The value range for the *virtual-router-id* argument is 1 to 255.

adver-interval: Specifies an interval for the master in the specified IPv4 VRRP group to send VRRP advertisements. The value range for this argument is 10 to 4095 centiseconds. For VRRPv2, the value of the *adver-interval* argument can only be a multiple of 100. For example, if you configure values in the range of 10 to 100, 101 to 200, and 4001 to 4095, the actual values are 100, 200, and 4100, respectively. For VRRPv3, the configured value for the *adver-interval* argument takes effect.

Usage guidelines

The master in an IPv4 VRRP group periodically sends VRRP advertisements to declare its presence. You can use this command to configure the interval at which the master sends VRRP advertisements.

As a best practice to maintain system stability, set the VRRP advertisement interval to be greater than 100 centiseconds.

In VRRPv2, all routers in an IPv4 VRRP group must have the same interval for sending VRRP advertisements.

In VRRPv3, the routers in an IPv4 VRRP group can have different intervals for sending VRRP advertisements. The master in the VRRP group sends VRRP advertisements at the specified interval and carries the interval attribute in the advertisements. After a backup receives the advertisement, it records the interval in the advertisement. If the backup does not receive any VRRP advertisement when the timer (3 × recorded interval + Skew_Time) expires, it regards the master as failed and takes over.

Large network traffic might disable a backup from receiving VRRP advertisements from the master within the specified timer and trigger an unexpected master switchover. To solve this problem, you can use this command to set a larger interval.

Examples

Configure the master in IPv4 VRRP group 1 to send VRRP advertisements at an interval of 500 centiseconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 timer advertise 500
```

Related commands

display vrrp

vrrp vrid track

Use **vrrp vrid track** to associate a VRRP group or the VFs in a VRRP group with a track entry.

Use **undo vrrp vrid track** to remove the association between a VRRP group or the VFs in a VRRP group and a track entry.

Syntax

vrrp vrid *virtual-router-id* **track** *track-entry-number* { **forwarder-switchover member-ip** *ip-address* | **priority reduced** [*priority-reduced*] | **switchover** | **weight reduced** [*weight-reduced*] }

undo vrrp vrid *virtual-router-id* **track** [*track-entry-number*] [**forwarder-switchover** | **priority reduced** | **switchover** | **weight reduced**]

Default

A VRRP group and the VFs in a VRRP group are not associated with any track entries.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group number. The value range for the *virtual-router-id* argument is 1 to 255.

track-entry-number: Specifies a track entry by its number in the range of 1 to 1024.

forwarder-switchover member-ip *ip-address*: Enables the LVF on the router to take over the role of the AVF at the specified IP address immediately after the specified track entry changes to the Negative state. The *ip-address* argument specifies the IP address of a member router. You can use the **display vrrp verbose** command to view the IP addresses of the members.

priority reduced [*priority-reduced*]: Reduces the priority of the router in the VRRP group by the specified value when the state of the specified track entry changes to Negative. The value range for the *priority-reduced* argument is 1 to 255, and the default value is 10.

switchover: Enables the router in backup state to take over as the master immediately after the specified track entry changes to the Negative state.

weight reduced [*weight-reduced*]: Reduces the weight of all VFs on the router in the VRRP group by the specified value when the state of the specified track entry changes to Negative. The value range for the *weight-reduced* argument is 1 to 255, and the default value is 30.

Usage guidelines

When the associated track entry changes to the Negative state, one of the following events occurs depending on your configuration:

- The priority of the router in the VRRP group decreases by a specified value.
- The weight of VFs decreases by a specified value.

- The router immediately takes over as the master if it is a backup.
- The LVF on the router immediately takes over the role of the AVF at the specified IP address.

When the track entry changes from Negative to Positive or NotReady, one of the following events occurs:

- The router automatically restores its priority or VF weight.
- The failed master router becomes the master again.
- The failed AVF becomes active again.

Before executing this command, create a VRRP group on the interface and assign a virtual IP address to the VRRP group.

You can create a track entry by using the **track** command before or after you associate it with a VRRP group or the VFs in a VRRP group. For more information about configuring track entries, see *High Availability Configuration Guide*.

If no track entry is specified, the **undo vrrp vrid track** command removes all associations between track entries and the VRRP group or VFs in the VRRP group.

The **vrrp vrid track priority reduced** command and the **vrrp vrid track switchover** command do not take effect on an IP address owner. If you configure the command on an IP address owner, the configuration takes effect after the router changes to be a non-IP address owner.

The following parameters take effect only when the IPv4 VRRP group is operating in load balancing mode:

- The **forwarder-switchover member-ip** *ip-address* option.
- The **weight reduced** *weight-reduced* option.
- The **weight reduced** keyword.

The weight of a VF is 255, and its lower limit of failure is 10.

When the weight of a VF owner is higher than or equal to the lower limit of failure, its priority is always 255. The priority does not change with the weight. When the upstream link of the VF owner fails, an LVF must take over as the AVF. The switchover occurs when the weight of the VF owner drops below the lower limit of failure. This requires that the reduced weight for the VF owner be higher than 245.

Examples

Associate VRRP group 1 on VLAN-interface 2 with track entry 1 and decrease the router priority by 50 when the state of track entry 1 changes to Negative.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 track 1 priority reduced 50
```

Associate the VFs of IPv4 VRRP group 1 on VLAN-interface 2 with track entry 1. Enable the LVF to take over the role of the AVF at the IP address of 10.1.1.3 immediately when the state of track entry 1 changes to Negative.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 track 1 forwarder-switchover member-ip 10.1.1.3
```

Associate the VFs of IPv4 VRRP group 1 on VLAN-interface 2 with track entry 1. Decrease the weight of all VFs on the router in the VRRP group by 50 when the state of track entry 1 changes to Negative.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 track 1 weight reduced 50
```

Related commands

display vrrp

vrrp vrid vrrpv3-send-packet

Use **vrrp vrid vrrpv3-send-packet** to set the packet sending mode for IPv4 VRRPv3.

Use **undo vrrp vrid vrrpv3-send-packet** to restore the default.

Syntax

vrrp vrid *virtual-router-id* **vrrpv3-send-packet** { **v2-only** | **v2v3-both** }

undo vrrp vrid *virtual-router-id* **vrrpv3-send-packet**

Default

A router configured with IPv4 VRRPv3 sends only VRRPv3 packets.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID. The value range for the *virtual-router-id* argument is 1 to 255.

v2-only: Sends VRRPv2 packets only.

v2v3-both: Sends both VRRPv2 and VRRPv3 packets.

Usage guidelines

This command takes effect only on IPv4 VRRPv3.

The packet sending mode for IPv4 VRRPv3 takes effect only on outgoing VRRP packets. A router configured with VRRPv3 can process incoming VRRPv2 and VRRPv3 packets.

If you set the packet sending mode for IPv4 VRRPv3 and configure VRRP packet authentication, authentication information will be carried in outgoing VRRPv2 packets but not in outgoing VRRPv3 packets.

The VRRP advertisement interval is set in centiseconds by using the **vrrp vrid timer advertise** command. The VRRP advertisement interval carried in VRRPv2 packets sent from routers configured with VRRPv3 might be different from the configured value. For information about the VRRP advertisement interval, see the **vrrp vrid timer advertise** command.

Examples

Configure VRRP group 1 to send both VRRPv2 and VRRPv3 packets.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 vrrpv3-send-packet v2v3-both
```

Related commands

display vrrp

vrrp vrid timer advertise

IPv6 VRRP commands

display vrrp ipv6

Use **display vrrp ipv6** to display the states of IPv6 VRRP groups.

Syntax

display vrrp ipv6 [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

vrid *virtual-router-id*: Specifies an IPv6 VRRP group by its virtual router ID. The value range for the *virtual-router-id* argument is 1 to 255.

verbose: Displays detailed IPv6 VRRP group information. If you do not specify the **verbose** keyword, the command displays brief IPv6 VRRP group information.

Usage guidelines

If no interface or VRRP group is specified, this command displays the states of all IPv6 VRRP groups.

If only an interface is specified, this command displays the states of all IPv6 VRRP groups on the specified interface.

If both an interface and an IPv6 VRRP group are specified, this command displays the states of the specified IPv6 VRRP group on the specified interface.

Examples

Display brief information about all IPv6 VRRP groups on the device when VRRP operates in standard mode.

```
<Sysname> display vrrp ipv6
IPv6 Virtual Router Information:
 Running Mode      : Standard
 ND sending interval : 120 sec
 Total number of virtual routers : 1
 Interface          VRID  State        Running Adver   Auth     Virtual
                                       Pri     Timer   Type        IP
 ------------------------------------------------------------------------
 Vlan2              1     Master       150     100     None     FE80::1
```

Table 8 Command output (in standard mode)

Field	Description
Running Mode	VRRP operating mode (standard mode).

Field	Description
ND sending interval	Sending interval for ND packets. This field is displayed only after you configure the **vrrp ipv6 send-nd** command.
Total number of virtual routers	Total number of VRRP groups.
Interface	Interface where the VRRP group is configured.
VRID	Virtual router ID (VRRP group number).
State	State of the router in the VRRP group: • **Master**—The router is the master in the VRRP group. • **Backup**—The router is the backup in the VRRP group. • **Initialize**—The router is in **Initialize** state. • **Inactive**—The router is in **Inactive** state, for example, when the router is not assigned a virtual IP address by using the **vrrp vrid** command.
Running Pri	Current priority of the router. When a track entry is associated with a VRRP group on the router, the router's priority changes when the track entry's status changes.
Adver Timer	VRRP advertisement sending interval in centiseconds.
Auth Type	Authentication type. Only **none** is available, which means no authentication is required.
Virtual IP	Virtual IP address of the VRRP group.

Display detailed information about all IPv6 VRRP groups on the device when VRRP operates in standard mode.

```
<Sysname> display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode      : Standard
 ND sending interval : 120 sec
 Total number of virtual routers : 2
   Interface Vlan-interface2
     VRID             : 1                  Adver Timer  : 100
     Admin Status     : Up                 State        : Master
     Config Pri       : 150                Running Pri  : 150
     Preempt Mode     : Yes                Delay Time   : 10
     Auth Type        : None
     Virtual IP       : FE80::1
     Virtual MAC      : 0000-5e00-0201
     Master IP        : FE80::2
     Config Role      : Master
     Name             : abc
   VRRP Track Information:
     Track Object   : 1                  State : Positive   Pri Reduced : 50

   Interface Vlan-interface2
     VRID             : 2                  Adver Timer  : 100
     Admin Status     : Up                 State        : Backup
     Config Pri       : 80                 Running Pri  : 80
     Preempt Mode     : Yes                Delay Time   : 0
```

```
  Become Master    : 2450ms left
  Auth Type        : None
  Virtual IP       : FE80::11
  Virtual MAC      : 0000-5e00-0202
  Master IP        : FE80::12

Interface Vlan-interface2
  VRID             : 3                   Adver Timer  : 100
  Admin Status     : Up                  State        : Master
  Config Pri       : 100                 Running Pri  : 100
  Preempt Mode     : Yes                 Delay Time   : 0
  Auth Type        : None
  Virtual IP       : FE80::10
  Virtual MAC      : 0000-5e00-0203
  Master IP        : FE80::2
  Config Role      : Subordinate
  Follow Name      : abc
```

Table 9 Command output (in standard mode)

Field	Description
Running Mode	VRRP operating mode (standard mode).
ND sending interval	Sending interval for ND packets. This field is displayed only after you configure the **vrrp ipv6 send-nd** command.
Total number of virtual routers	Total number of VRRP groups.
Interface	Interface where the VRRP group is configured.
VRID	Virtual router ID (VRRP group number).
Adver Timer	VRRP advertisement sending interval in centiseconds.
Admin Status	Administrative status: **Up** or **Down**.
State	State of the router in the VRRP group: • **Master**—The router is the master in the VRRP group. • **Backup**—The router is the backup in the VRRP group. • **Initialize**—The router is in **Initialize** state. • **Inactive**—The router is in **Inactive** state, for example, when the router is not assigned a virtual IP address by using the **vrrp vrid** command.
Config Pri	Configured priority of the router, which is configured by using the **vrrp ipv6 vrid priority** command.
Running Pri	Current priority of the router. When a track entry is associated with a VRRP group on the router, the router's priority changes when the track entry's status changes.
Preempt Mode	Preemptive mode: • **Yes**. • **No**.
Delay Time	Preemption delay in centiseconds.
Become Master	Time (in milliseconds) that a backup router has to wait before it becomes the master. This field is displayed only when the router is a backup.

Field	Description
Auth Type	Authentication type. Only **none** is available, which means no authentication is required.
Virtual IP	Virtual IP address of the VRRP group.
Virtual MAC	Virtual MAC address of the VRRP group's virtual IP address, which is displayed when the router is the master.
Master IP	Link-local address of the interface where the master resides.
Config Role	The configured role of the IPv6 VRRP group to which the router belongs. • **Master**. • **Subordinate**.
Name	Master group name assigned to the IPv6 VRRP group. This field is displayed only after you configure the **vrrp ipv6 vrid name** command.
Follow Name	Name of the master VRRP group that the IPv6 VRRP group follows. This field is displayed only after you configure the **vrrp ipv6 vrid follow** command.
VRRP Track Information	Track entry information. This field is displayed only after you configure the **vrrp ipv6 vrid track** command.
Track Object	Track entry which is associated with the VRRP group.
State	Track entry state: • **Negative**. • **Positive**. • **NotReady**.
Pri Reduced	Value by which the priority decreases when the state of the associated track entry becomes Negative.
Switchover	Switchover mode. When the state of the associated track entry becomes Negative, the backup immediately becomes the master.

Display brief information about all IPv6 VRRP groups on the device when VRRP operates in load balancing mode.

```
<Sysname> display vrrp ipv6
IPv6 Virtual Router Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 1
 Interface          VRID  State        Running Address             Active
                                       Pri
 ------------------------------------------------------------------------
 Vlan2              1     Master       150     FE80::1             Local
 -----              VF1   Active       255     000f-e2ff-4011      Local
```

Table 10 Command output (in load balancing mode)

Field	Description
Running Mode	VRRP operating mode (load balancing mode).
Total number of virtual routers	Total number of VRRP groups.
Interface	Interface where the VRRP group is configured.
VRID	Virtual router ID (VRRP group number) or VF ID.

Field	Description

State	• For a VRRP group, this field indicates the state of the router in the VRRP group:
	  ○ **Master**—The router is the master in the VRRP group.
	  ○ **Backup**—The router is the backup in the VRRP group.
	  ○ **Initialize**—The router is in **Initialize** state.
	  ○ **Inactive**—The router is in **Inactive** state, for example, when the router is not assigned a virtual IP address by using the **vrrp vrid** command.
	• For a VF, this field indicates the state of the VF in the VRRP group:
	  ○ **Active**—The VF is created on the device.
	  ○ **Listening**—The VF is learned from another device.
	  ○ **Initialize**—The VF is in **Initialize** state.

Running Pri	• For a VRRP group, this field indicates the running priority of the router. When a track entry is associated with a VRRP group on the router, the router's priority changes when the track entry's status changes. • For a VF, this field indicates the running priority of the VF. When a track entry is associated with a VF, the priority of the VF changes if the state of the track entry changes.
Address	• For a VRRP group, this field indicates the virtual IP address of the VRRP group. • For a VF, this field indicates the virtual MAC address of the VF.
Active	• For a VRRP group, this field indicates the link-local address of the interface where the master resides. If the current router is the master, this field displays **local**. • For a VF, this field indicates the link-local address of the interface where the AVF resides. If the current VF is the AVF, this field displays **local**.

Display detailed information about all IPv6 VRRP groups on the device when VRRP operates in load balancing mode.

```
<Sysname> display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 2
   Interface Vlan-interface2
     VRID           : 1                   Adver Timer  : 100
     Admin Status   : Up                  State        : Master
     Config Pri     : 150                 Running Pri  : 150
     Preempt Mode   : Yes                 Delay Time   : 5
     Auth Type      : None
     Virtual IP     : FE80::10
     Member IP List : FE80::3 (Local, Master)
                      FE80::2 (Backup)
     Master IP      : FE80::3
   VRRP Track Information:
     Track Object   : 1                   State : Positive   Pri Reduced : 50
   Forwarder Information: 2 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 01
```

```
  State          : Active
  Virtual MAC    : 000f-e2ff-4011 (Owner)
  Owner ID       : 0000-5e01-1101
  Priority       : 255
  Active         : local
 Forwarder 02
  State          : Listening
  Virtual MAC    : 000f-e2ff-4012 (Learnt)
  Owner ID       : 0000-5e01-1103
  Priority       : 127
  Active         : FE80::2
Forwarder Weight Track Information:
  Track Object   : 1          State : Positive   Weight Reduced : 250
Interface Vlan-interface2
  VRID           : 11                  Adver Timer  : 100
  Admin Status   : Up                  State        : Backup
  Config Pri     : 80                  Running Pri  : 80
  Preempt Mode   : Yes                 Delay Time   : 0
  Become Master  : 2450ms left
  Auth Type      : None
  Virtual IP     : FE80::11
  Member IP List : FE80::3 (Local, Backup)
                   FE80::2 (Master)
  Master IP      : FE80::2
Forwarder Information: 2 Forwarders 1 Active
  Config Weight  : 255
  Running Weight : 255
 Forwarder 01
  State          : Active
  Virtual MAC    : 000f-e2ff-40b1 (Learnt)
  Owner ID       : 0000-5e01-1103
  Priority       : 127
  Active         : FE80::2
 Forwarder 02
  State          : Listening
  Virtual MAC    : 000f-e2ff-40b2 (Owner)
  Owner ID       : 0000-5e01-1101
  Priority       : 255
  Active         : local
```

Table 11 Command output (in load balancing mode)

Field	Description
Running Mode	VRRP operating mode (load balancing mode).
Total number of virtual routers	Total number of VRRP groups.
Interface	Interface where the VRRP group is configured.
VRID	Virtual router ID (VRRP group number).
Adver Timer	VRRP advertisement sending interval in centiseconds.

Field	Description
Admin Status	Administrative status: **Up** or **Down**.
State	State of the router in the VRRP group: • **Master**—The router is the master in the VRRP group. • **Backup**—The router is the backup in the VRRP group. • **Initialize**—The router is in **Initialize** state. • **Inactive**—The router is in **Inactive** state, for example, when the router is not assigned a virtual IP address by using the **vrrp vrid** command.
Config Pri	Configured priority of the router, which is configured by using the **vrrp ipv6 vrid priority** command.
Running Pri	Current priority of the router. When a track entry is associated with a VRRP group on the router, the router's priority changes when the track entry's status changes.
Preempt Mode	Preemptive mode: • **Yes**. • **No**.
Delay Time	Preemption delay in centiseconds.
Become Master	Time (in milliseconds) that a backup router has to wait before it becomes the master. This field is displayed only when the router is a backup.
Auth Type	Authentication type. Only **none** is available, which means no authentication is required.
Virtual IP	Virtual IP address list of the VRRP group.
Member IP List	IP addresses of the member devices in the VRRP group: • **Local**—IP address of the local router. • **Master**—IP address of the master. • **Backup**—IP address of the backup.
VRRP Track Information	Track entry that is associated with the VRRP group. This field is displayed only after you configure the **vrrp ipv6 vrid track** command.
Track Object	Track entry to be monitored. This field is displayed only after you configure the **vrrp ipv6 vrid track** command.
State	Track entry state: • **Negative**. • **Positive**. • **NotReady**.
Pri Reduced	Value by which the priority decreases when the status of the associated track entry becomes Negative. This field is displayed only after you configure the **vrrp ipv6 vrid track** command.
Switchover	Switchover mode. When the status of the associated track entry becomes Negative, the backup immediately becomes the master.
Forwarder Information: 2 Forwarders 1 Active	VF information: Two VFs exist and one is the AVF.
Config Weight	Configured weight of the VF: 255.
Running Weight	Current weight of the VF. When a track entry is associated with the VFs of a VRRP group, the VFs' weights change when the track entry's status changes.

Field	Description
Forwarder 01	Information about VF 01.
State	VF state: • **Active**—The VF is created on the device. • **Listening**—The VF is learned from another device. • **Initialize**—The VF is in **Initialize** state.
Virtual MAC	Virtual MAC address of the VF.
Owner ID	Real MAC address of the VF owner.
Priority	VF priority in the range of 1 to 255.
Active	Link-local address of the interface where the AVF resides. If the current VF is the AVF, this field displays **local**.
Forwarder Weight Track Configuration	VF weight Track configuration. The field is displayed only after you configure the **vrrp ipv6 vrid track** command.
Track Object	Track entry which is associated with the VFs. The field is displayed only after you configure the **vrrp ipv6 vrid track** command.
State	Track entry state: • **Negative**. • **Positive**. • **NotReady**.
Weight Reduced	Value by which the weights of the VFs decrease when the state of the associated track entry changes to Negative. The field is displayed only after you configure the **vrrp ipv6 vrid track** command.
Forwarder Switchover Track Information:	VF switchover Track configuration. The field is displayed only after you configure the **vrrp ipv6 vrid track** command.
Member IP	IPv6 address of a member device. The field is displayed only after you configure the **vrrp ipv6 vrid track** command.

display vrrp ipv6 binding

Use **display vrrp ipv6 binding** to display master-to-subordinate IPv6 VRRP group bindings.

Syntax

display vrrp ipv6 binding [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*] | **name** *name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. The interface must be an interface to which master IPv6 VRRP groups belong.

vrid *virtual-router-id*: Specifies a master IPv6 VRRP group by its virtual router ID. The value range for the *virtual-router-id* argument is 1 to 255.

name *name*: Specifies a master IPv6 VRRP group by its name, a case-sensitive string of 1 to 20 characters.

Usage guidelines

If you do not specify any parameters, this command displays all master-to-subordinate IPv6 VRRP group bindings.

If you specify an interface but do not specify the virtual router ID of a master IPv6 VRRP group, this command displays all master-to-subordinate IPv6 VRRP group bindings on the specified interface.

If you specify an interface and the virtual router ID of a master IPv6 VRRP group, this command displays the binding information about the specified master VRRP group on the specified interface.

Examples

Display master-to-subordinate IPv6 VRRP group bindings.

```
<Sysname> display vrrp ipv6 binding
IPv6 virtual router binding information:
  Total number of master virtual routers            : 1
  Total number of subordinate virtual routers       : 2
  Interface : Vlan2                    Master VRID : 1
  Name      : a                        Status      : Backup
  Subordinate virtual routers : 1
    Interface : Vlan2                  VRID        : 4

  Interface : --                       Master VRID : --
  Name      : c                        Status      : --
  Subordinate virtual routers : 1
    Interface : Vlan2                  VRID        : 5
```

Table 12 Command output

Field	Description
Total number of master virtual routers	Total number of master IPv6 VRRP groups.
Total number of subordinate virtual routers	Total number of subordinate IPv6 VRRP groups.
Interface	Interface to which the master IPv6 VRRP group belongs. If the master IPv6 VRRP group does not exist, this field displays two hyphens (**--**).
Master VRID	Virtual router ID of the master IPv6 VRRP group. If the master IPv6 VRRP group does not exist, this field displays two hyphens (**--**).
Name	Name of the master IPv6 VRRP group.
Status	Status of the router in the master IPv6 VRRP group: • **Master**. • **Backup**. • **Initialize**. • **Inactive**.

Field	Description
	If the master IPv6 VRRP group does not exist, this field displays two hyphens (**--**).
Subordinate virtual routers	Number of subordinate IPv6 VRRP groups.
Interface	Interface to which the subordinate IPv6 VRRP group belongs.
VRID	Virtual router ID of the subordinate IPv6 VRRP group.

Related commands

vrrp ipv6 vrid follow

vrrp ipv6 vrid name

display vrrp ipv6 statistics

Use **display vrrp ipv6 statistics** to display statistics for IPv6 VRRP groups.

Syntax

display vrrp ipv6 statistics [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

vrid *virtual-router-id*: Specifies an IPv6 VRRP group by its virtual router ID. The value range for the *virtual-router-id* argument is 1 to 255.

Usage guidelines

If no interface or VRRP group is specified, this command displays statistics for all IPv6 VRRP groups.

If only an interface is specified, this command displays statistics for all IPv6 VRRP groups on the specified interface.

If both an interface and an IPv6 VRRP group are specified, this command displays statistics for the specified IPv6 VRRP group on the specified interface.

Examples

Display statistics for all IPv6 VRRP groups when VRRP operates in standard mode.

```
<Sysname> display vrrp ipv6 statistics
 Interface              : Vlan-interface2
 VRID                   : 1
 CheckSum Errors        : 0          Version Errors               : 0
 Invalid Pkts Rcvd      : 0          Unexpected Pkts Rcvd         : 0
 Hop Limit Errors       : 0          Advertisement Interval Errors : 0
 Invalid Auth Type      : 0          Auth Failures                : 0
```

```
 Packet Length Errors    : 0          Auth Type Mismatch           : 0
 Become Master           : 1          Address List Errors          : 0
 Adver Rcvd              : 0          Priority Zero Pkts Rcvd      : 0
 Adver Sent              : 425        Priority Zero Pkts Sent      : 0
IP Owner Conflicts      : 0

 Global statistics
 CheckSum Errors         : 0
 Version Errors          : 0
 VRID Errors             : 0
```

Display statistics for all IPv6 VRRP groups when VRRP operates in load balancing mode.

```
<Sysname> display vrrp ipv6 statistics
 Interface               : Vlan-interface2
 VRID                    : 1
 CheckSum Errors         : 0          Version Errors               : 0
 Invalid Pkts Rcvd       : 0          Unexpected Pkts Rcvd         : 0
 Hop Limit Errors        : 0          Advertisement Interval Errors : 0
 Invalid Auth Type       : 0          Auth Failures                : 0
 Packet Length Errors    : 0          Auth Type Mismatch           : 0
 Become Master           : 39         Address List Errors          : 0
 Become AVF              : 13         Packet Option Errors         : 0
 Adver Rcvd              : 2562       Priority Zero Pkts Rcvd      : 1
 Adver Sent              : 16373      Priority Zero Pkts Sent      : 49
 Request Rcvd            : 2          Reply Rcvd                   : 10
 Request Sent            : 12         Reply Sent                   : 2
 Release Rcvd            : 0          VF Priority Zero Pkts Rcvd   : 1
 Release Sent            : 0          VF Priority Zero Pkts Sent   : 11
 Redirect Timer Expires  : 1          Time-out Timer Expires       : 0

 Global statistics
 CheckSum Errors         : 0
 Version Errors          : 0
 VRID Errors             : 0
```

Table 13 Command output (in standard mode)

Field	Description
Interface	Interface where the VRRP group is configured.
VRID	VRRP group number.
CheckSum Errors	Number of packets with checksum errors.
Version Errors	Number of packets with version errors.
Invalid Pkts Rcvd	Number of received packets of invalid packet types.
Unexpected Pkts Rcvd	Number of received unexpected packets.
Advertisement Interval Errors	Number of packets with advertisement interval errors.
Hop Limit Errors	Number of packets with hop limit errors.
Auth Failures	Number of packets with authentication failures.

Field	Description
Invalid Auth Type	Number of packets with authentication failures because of invalid authentication types.
Auth Type Mismatch	Number of packets with authentication failures because of mismatching authentication types.
Packet Length Errors	Number of packets with VRRP packet length errors.
Address List Errors	Number of packets with virtual IP address list errors.
Become Master	Number of times that the router has been elected as the master.
Priority Zero Pkts Rcvd	Number of received advertisements with the router priority of 0.
Adver Rcvd	Number of received advertisements.
Priority Zero Pkts Sent	Number of sent advertisements with the router priority of 0.
Adver Sent	Number of sent advertisements.
IP Owner Conflicts	Number of VRRP packets that the local router (IP address owner) has received from conflicting IP address owners.
Global statistics	Global statistics for all IPv6 VRRP groups.
CheckSum Errors	Total number of packets with checksum errors.
Version Errors	Total number of packets with version errors.
VRID Errors	Total number of packets with VRID errors.

Table 14 Command output (in load balancing mode)

Field	Description
Interface	Interface where the VRRP group is configured.
VRID	VRRP group number.
CheckSum Errors	Number of packets with checksum errors.
Version Errors	Number of packets with version errors.
Invalid Pkts Rcvd	Number of received packets of invalid packet types.
Unexpected Pkts Rcvd	Number of received unexpected packets.
Advertisement Interval Errors	Number of packets with advertisement interval errors.
Hop Limit Errors	Number of packets with hop limit errors.
Auth Failures	Number of packets with authentication failures.
Invalid Auth Type	Number of packets with authentication failures because of invalid authentication types.
Auth Type Mismatch	Number of packets with authentication failures because of mismatching authentication types.
Packet Length Errors	Number of packets with VRRP packet length errors.
Address List Errors	Number of packets with virtual IP address list errors.
Become Master	Number of times that the router has been elected as the master.
Redirect Timer Expires	Number of times that the redirect timer expired.

Field	Description
Become AVF	Number of times that the VF has been elected as the AVF.
Time-out Timer Expires	Number of times that the time-out timer expired.
Adver Rcvd	Number of received advertisements.
Request Rcvd	Number of received requests.
Adver Sent	Number of sent advertisements.
Request Sent	Number of sent requests.
Reply Rcvd	Number of received replies.
Release Rcvd	Number of received release packets.
Reply Sent	Number of sent replies.
Release Sent	Number of sent release packets.
Priority Zero Pkts Rcvd	Number of received advertisements with the router priority of 0.
VF Priority Zero Pkts Rcvd	Number of received advertisements with the VF priority of 0.
Priority Zero Pkts Sent	Number of sent advertisements with the router priority of 0.
VF Priority Zero Pkts Sent	Number of sent advertisements with the VF priority of 0.
Packet Option Errors	Number of packet option errors.
Global statistics	Global statistics for all IPv6 VRRP groups.
CheckSum Errors	Total number of packets with checksum errors.
Version Errors	Total number of packets with version errors.
VRID Errors	Total number of packets with VRID errors.

Related commands

`reset vrrp ipv6 statistics`

reset vrrp ipv6 statistics

Use **`reset vrrp ipv6 statistics`** to clear statistics for IPv6 VRRP groups.

Syntax

`reset vrrp ipv6 statistics` [**`interface`** *`interface-type interface-number`* [**`vrid`** *`virtual-router-id`*]]

Views

User view

Predefined user roles

network-admin

Parameters

`interface` *`interface-type interface-number`*: Specifies an interface by its type and number.

`vrid` *`virtual-router-id`*: Specifies an IPv6 VRRP group by its virtual router ID. The value range for the *`virtual-router-id`* argument is 1 to 255.

Usage guidelines

If no interface or VRRP group is specified, this command clears statistics for all IPv6 VRRP groups.

If only an interface is specified, this command clears statistics for all IPv6 VRRP groups on the specified interface.

If both an interface and an IPv6 VRRP group are specified, this command clears statistics for the specified IPv6 VRRP group on the specified interface.

Examples

Clear statistics for all IPv6 VRRP groups on all interfaces.

```
<Sysname> reset vrrp ipv6 statistics
```

Related commands

display vrrp ipv6 statistics

vrrp ipv6 dscp

Use **vrrp ipv6 dscp** to set a DSCP value for IPv6 VRRP packets.

Use **undo vrrp ipv6 dscp** to restore the default.

Syntax

vrrp ipv6 dscp *dscp-value*

undo vrrp ipv6 dscp

Default

The DSCP value for IPv6 VRRP packets is 56.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies a DSCP value for IPv6 VRRP packets, in the range of 0 to 63.

Usage guidelines

The DSCP value identifies the packet priority during transmission. A greater DSCP value means a higher packet priority.

Examples

Set the DSCP value to 30 for IPv6 VRRP packets.

```
<Sysname> system-view
[Sysname] vrrp ipv6 dscp 30
```

vrrp ipv6 mode

Use **vrrp ipv6 mode** to specify the operating mode for IPv6 VRRP.

Use **undo vrrp ipv6 mode** to restore the default.

Syntax

vrrp ipv6 mode load-balance

undo vrrp ipv6 mode

Default

IPv6 VRRP operates in standard mode.

Views

System view

Predefined user roles

network-admin

Parameters

load-balance: Specifies the load balancing mode.

Usage guidelines

For IPv6 VRRP to operate correctly in load balancing mode, make sure the virtual IPv6 address of an IPv6 VRRP group is not the IPv6 address of any interfaces in the VRRP group.

After you create IPv6 VRRP groups on the router, you can use this command to modify their operating mode. All IPv6 VRRP groups on the router operate in the specified mode.

Examples

Specify the load balancing mode for IPv6 VRRP.

```
<Sysname> system-view
[Sysname] vrrp ipv6 mode load-balance
```

Related commands

display vrrp ipv6

vrrp ipv6 send-nd

Use **vrrp ipv6 send-nd** to enable periodic sending of ND packets for IPv6 VRRP.

Use **undo vrrp ipv6 send-nd** to disable periodic sending of ND packets for IPv6 VRRP.

Syntax

vrrp ipv6 send-nd [**interval** *interval*]

undo vrrp ipv6 send-nd

Default

Periodic sending of ND packets is disabled for IPv6 VRRP.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the sending interval in the range of 30 to 1200 seconds. The default value is 120 seconds.

Usage guidelines

This command ensures that the MAC address entry for the virtual MAC address of an IPv6 VRRP group can be updated on downstream devices in a timely manner.

This command takes effect only in VRRP standard mode.

If you change the sending interval for ND packets, the configuration takes effect at the next sending interval.

The master sends the first ND packet at a random time in the second half of the set interval after you execute the **vrrp ipv6 send-nd** command. This prevents too many ND packets from being sent at the same time.

The sending interval for ND packets might be much longer than the set interval when the following conditions are met:

- Multiple IPv6 VRRP groups exist on the device.
- A short sending interval is set.

Examples

Enable periodic sending of ND packets for IPv6 VRRP and set the sending interval to 200 seconds.

```
<Sysname> system-view
[Sysname] vrrp ipv6 send-nd interval 200
```

vrrp ipv6 vrid

Use **vrrp ipv6 vrid** to create an IPv6 VRRP group and assign a virtual IPv6 address to it, or to assign a virtual IPv6 address to an existing IPv6 VRRP group.

Use **undo vrrp ipv6 vrid** to remove all configurations of an IPv6 VRRP group, or to remove a virtual IPv6 address from an IPv6 VRRP group.

Syntax

vrrp ipv6 vrid *virtual-router-id* **virtual-ip** *virtual-address* [**link-local**]

undo vrrp ipv6 vrid *virtual-router-id* [**virtual-ip** [*virtual-address* [**link-local**]]]

Default

No IPv6 VRRP groups exist.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group by its virtual router ID. The value range for the *virtual-router-id* argument is 1 to 255.

virtual-ip *virtual-address*: Specifies a virtual IPv6 address. If you do not specify this option, the **undo vrrp ipv6 vrid** command removes all virtual IPv6 addresses from the specified IPv6 VRRP group.

link-local: Specifies a link-local address as the virtual IPv6 address.

Usage guidelines

You can execute this command multiple times to assign multiple virtual IPv6 addresses to an IPv6 VRRP group. An IPv6 VRRP group can have a maximum of 16 virtual IPv6 addresses.

The first virtual IPv6 address that you assign to an IPv6 VRRP group must be a link-local address, and it must be removed last.

An IPv6 VRRP group can have only one link-local address as its virtual IPv6 address.

An IPv6 VRRP group without virtual IPv6 addresses configured can exist on a device provided that other settings (for example, priority and preemption mode) are available. Such a VRRP group stays in inactive state and does not function.

The virtual IPv6 address of an IPv6 VRRP group and the downlink interface IPv6 address of the VRRP group members must be in the same subnet. Otherwise, the hosts in the subnet might fail to access external networks.

Examples

Create IPv6 VRRP group 1 and assign virtual IPv6 address fe80::10 to the VRRP group. Then assign virtual IPv6 address 1::10 to the VRRP group.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

Related commands

display vrrp ipv6

vrrp ipv6 vrid follow

Use **vrrp ipv6 vrid follow** to configure an IPv6 VRRP group to follow a master group.

Use **undo vrrp ipv6 vrid follow** to remove the configuration.

Syntax

vrrp ipv6 vrid *virtual-router-id* **follow** *name*

undo vrrp ipv6 vrid *virtual-router-id* **follow**

Default

An IPv6 VRRP group does not follow a master group.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group by its virtual router ID. The value range for the *virtual-router-id* argument is 1 to 255.

name: Specifies a master IPv6 VRRP group by its name, a case-sensitive string of 1 to 20 characters.

Usage guidelines

This command configures an IPv6 VRRP group as a subordinate VRRP group to follow a master group. A subordinate IPv6 VRRP group can forward service traffic.

An IPv6 VRRP group cannot be both a master group and a subordinate group.

An IPv6 VRRP group stays in **Inactive** state if it is configured to follow a nonexistent master VRRP group.

If an IPv6 VRRP group in **Inactive** or **Initialize** state follows a master group that is not in **Inactive** state, the state of the VRRP group does not change.

Examples

Configure IPv6 VRRP group 1 to follow master group **abc**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 follow abc
```

Related commands

display vrrp ipv6 binding

vrrp ipv6 vrid name

vrrp ipv6 vrid name

Use **vrrp ipv6 vrid name** to configure an IPv6 VRRP group as a master group and assign a name to it.

Use **undo vrrp ipv6 vrid name** to remove the configuration.

Syntax

vrrp ipv6 vrid *virtual-router-id* **name** *name*

undo vrrp ipv6 vrid *virtual-router-id* **name**

Default

An IPv6 VRRP group does not act as a master group.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group by its virtual router ID. The value range for the *virtual-router-id* argument is 1 to 255.

name: Specifies a master IPv6 VRRP group name, a case-sensitive string of 1 to 20 characters.

Usage guidelines

This command configures an IPv6 VRRP group as a master group through assigning a master group name to it. An IPv6 VRRP group that follows the master group is a subordinate VRRP group. The master VRRP group exchanges VRRP packets among member devices. The subordinate group does not exchange VRRP packets and follows the state of the master group. Both the master and subordinate VRRP groups can forward service traffic.

You cannot assign the same master VRRP group name to different IPv6 VRRP groups on a device.

Examples

Configure IPv6 VRRP group 1 as a master VRRP group and assign master group name **abc** to it.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 name abc
```

Related commands

display vrrp ipv6 binding

vrrp ipv6 vrid follow

vrrp ipv6 vrid preempt-mode

Use **vrrp ipv6 vrid preempt-mode** to enable the preemptive mode for the router in an IPv6 VRRP group and set the preemption delay.

Use **undo vrrp ipv6 vrid preempt-mode** to disable the preemptive mode for the router in an IPv6 VRRP group.

Use **undo vrrp ipv6 vrid preempt-mode delay** to restore the default preemption delay.

Syntax

vrrp ipv6 vrid *virtual-router-id* **preempt-mode** [**delay** *delay-value*]

undo vrrp ipv6 vrid *virtual-router-id* **preempt-mode** [**delay**]

Default

The router operates in preemptive mode and the preemption delay is 0 centiseconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group by its virtual router ID. The value range for the *virtual-router-id* argument is 1 to 255.

delay *delay-value*: Specifies the preemption delay in the range of 0 to 180000 in centiseconds.

Usage guidelines

In non-preemptive mode, the master router acts as the master as long as it operates correctly, even if a backup is assigned a higher priority later. The non-preemptive mode helps avoid frequent switchover between the master and backups.

In preemptive mode, a backup sends VRRP advertisements when it detects that it has a higher priority than the master. Then the backup takes over as the master and the previous master becomes a backup. This mechanism ensures that the master is always the router with the highest priority.

You can configure the VRRP preemption delay for the following purposes:

- Avoid frequent state changes among members in a VRRP group.
- Provide the backups with enough time to collect information (such as routing information).

A backup does not immediately become the master after it receives an advertisement with a lower priority than the local priority. Instead, it waits for a period of time before taking over.

Examples

Enable the preemptive mode for VRRP group 1, and set the preemption delay to 5000 centiseconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 10 preempt-mode delay 5000
```

Related commands

display vrrp ipv6

vrrp ipv6 vrid priority

Use **vrrp ipv6 vrid priority** to set the priority of the router in an IPv6 VRRP group.

Use **undo vrrp ipv6 vrid priority** to restore the default.

Syntax

vrrp ipv6 vrid *virtual-router-id* **priority** *priority-value*

undo vrrp ipv6 vrid *virtual-router-id* **priority**

Default

The priority of a router in an IPv6 VRRP group is 100.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group by its virtual router ID. The value range for the *virtual-router-id* argument is 1 to 255.

priority-value: Specifies a priority value in the range of 1 to 254. A higher value indicates a higher priority.

Usage guidelines

VRRP determines the role (master or backup) of each router in a VRRP group by priority. A router with a higher priority is more likely to become the master.

Priorities 1 to 254 are configurable. Priority 0 is reserved for special uses, and priority 255 is for the IP address owner. The IP address owner in a VRRP group always has a running priority of 255 and acts as the master as long as it operates correctly.

Examples

Set the priority of the switch to 150 in VRRP group 1 on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 priority 150
```

Related commands

display vrrp ipv6

vrrp ipv6 vrid shutdown

Use **vrrp ipv6 vrid shutdown** to disable an IPv6 VRRP group.

Use **undo vrrp ipv6 vrid shutdown** to enable an IPv6 VRRP group.

Syntax

vrrp ipv6 vrid *virtual-router-id* **shutdown**

undo vrrp ipv6 vrid *virtual-router-id* **shutdown**

Default

An IPv6 VRRP group is enabled.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group by its virtual router ID. The value range for the *virtual-router-id* argument is 1 to 255.

Usage guidelines

You can use this command to temporarily disable an IPv6 VRRP group. After this command is configured, the VRRP group stays in **Initialize** state, and its configurations remain unchanged. You can change the configuration of the VRRP group, and your changes take effect when you enable the VRRP group again.

Examples

Disable IPv6 VRRP group 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 shutdown
```

vrrp ipv6 vrid timer advertise

Use **vrrp ipv6 vrid timer advertise** to set the interval at which the master in an IPv6 VRRP group sends VRRP advertisements.

Use **undo vrrp ipv6 vrid timer advertise** to restore the default.

Syntax

vrrp ipv6 vrid *virtual-router-id* **timer advertise** *adver-interval*

undo vrrp ipv6 vrid *virtual-router-id* **timer advertise**

Default

The master in an IPv6 VRRP group sends VRRP advertisements at an interval of 100 centiseconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group by its virtual router ID. The value range for the *virtual-router-id* argument is 1 to 255.

adver-interval: Specifies an interval for the master in the specified IPv6 VRRP group to send VRRP advertisements, in the range of 100 to 4095 centiseconds.

Usage guidelines

The master in an IPv6 VRRP group periodically sends VRRP advertisements to declare its presence. You can use this command to set the interval at which the master sends VRRP advertisements.

As a best practice to maintain system stability, set the VRRP advertisement interval to be greater than 100 centiseconds.

The routers in an IPv6 VRRP group can have different intervals for sending VRRP advertisements. The master in the VRRP group sends VRRP advertisements at the specified interval and carries the interval attribute in the advertisements. After a backup receives the advertisement, it records the interval in the advertisement. If the backup does not receive any VRRP advertisement when the timer (3 × VRRP advertisement sending interval + Skew_Time) expires, it regards the master as failed and takes over.

Large network traffic might disable a backup from receiving VRRP advertisements from the master within the specified timer and trigger an unexpected master switchover. To solve this problem, you can use this command to configure a larger interval.

Examples

Configure the master in IPv6 VRRP group 1 to send VRRP advertisements at an interval of 500 centiseconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 timer advertise 500
```

Related commands

display vrrp ipv6

vrrp ipv6 vrid track

Use **vrrp ipv6 vrid track** to associate an IPv6 VRRP group or the VFs in an IPv6 VRRP group with a track entry.

Use **undo vrrp ipv6 vrid track** to remove the association between an IPv6 VRRP group or the VFs in an IPv6 VRRP group and a track entry.

Syntax

vrrp ipv6 vrid *virtual-router-id* **track** *track-entry-number* { **forwarder-switchover member-ip** *ipv6-address* | **priority reduced** [*priority-reduced*] | **switchover** | **weight reduced** [*weight-reduced*] }

undo vrrp ipv6 vrid *virtual-router-id* **track** [*track-entry-number*] [**forwarder-switchover** | **priority reduced** | **switchover** | **weight reduced**]]

Default

An IPv6 VRRP group and the VFs in an IPv6 VRRP group are not associated with any track entries.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group number. The value range for the *virtual-router-id* argument is 1 to 255.

track-entry-number: Specifies a track entry by its number in the range of 1 to 1024.

forwarder-switchover member-ip *ipv6-address*: Enables the LVF on the router to take over the role of the AVF at the specified IPv6 address immediately after the specified track entry changes to the Negative state. The *ipv6-address* argument specifies the IPv6 address of a member router. You can use the **display vrrp ipv6 verbose** command to view the IPv6 addresses of the members.

priority reduced [*priority-reduced*]: Reduces the priority of the router in the VRRP group by the specified value when the state of the specified track entry changes to Negative. The value range for the *priority-reduced* argument is 1 to 255, and the default value is 10.

switchover: Enables the router in backup state to take over as the master immediately after the specified track entry changes to the Negative state.

weight reduced [*weight-reduced*]: Reduces the weight of all VFs on the router in the VRRP group by the specified value when the state of the specified track entry changes to Negative. The value range for the *weight-reduced* argument is 1 to 255, and the default value is 30.

Usage guidelines

When the associated track entry changes to the Negative state, one of the following events occurs depending on your configuration:

- The priority of the router in the VRRP group decreases by a specified value.
- The weight of VFs decreases by a specified value.
- The router immediately takes over as the master if it is a backup.
- The LVF on the router immediately takes over the role of the AVF at the specified IPv6 address.

When the track entry changes from Negative to Positive or NotReady, one of the following events occurs:

- The router automatically restores its priority or VF weight.
- The failed master router becomes the master again.
- The failed AVF becomes active again.

Before executing this command, create an IPv6 VRRP group on the interface and assign a virtual IPv6 address to the IPv6 VRRP group.

You can create a track entry by using the **track** command before or after you associate it with an IPv6 VRRP group or the VFs in an IPv6 VRRP group. For more information about configuring track entries, see *High Availability Configuration Guide*.

If no track entry is specified, the **undo vrrp ipv6 vrid track** command removes all associations between track entries and the IPv6 VRRP group or VFs in the IPv6 VRRP group.

The **vrrp ipv6 vrid track priority reduced** command and the **vrrp ipv6 vrid track switchover** command do not take effect on an IP address owner. If you configure the command on an IP address owner, the configuration takes effect after the router changes to be a non-IP address owner.

The following parameters take effect only when the IPv6 VRRP group is operating in load balancing mode:

- The **forwarder-switchover member-ip** *ip-address* option.
- The **weight reduced** *weight-reduced* option.
- The **weight reduced** keyword.

The weight of a VF is 255, and its lower limit of failure is 10.

When the weight of a VF owner is higher than or equal to the lower limit of failure, its priority is always 255. The priority does not change with the weight. When the upstream link of the VF owner fails, an LVF must take over as the AVF. The switchover happens when the weight of the VF owner drops below the lower limit of failure. This requires that the reduced weight for the VF owner be higher than 245.

Examples

Associate IPv6 VRRP group 1 on VLAN-interface 2 with track entry 1 and decrease the router priority by 50 when the state of track entry 1 changes to Negative.

```
<Sysname> system-view
```

```
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 track 1 priority reduced 50
```

Associate the VFs of IPv6 VRRP group 1 on VLAN-interface 2 with track entry 1. Enable the LVF to take over the role of the AVF at the IPv6 address of 1::3 immediately when the state of track entry 1 changes to Negative.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 track 1 forwarder-switchover member-ip 1::3
```

Associate the VFs of IPv6 VRRP group 1 on VLAN-interface 2 with track entry 1. Decrease the weight of all VFs on the router in the VRRP group by 50 when the state of track entry 1 changes to Negative.

```
<Sysname> system-view
[Sysname] interface vlan-interface2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 track 1 weight reduced 50
```

Related commands

display vrrp ipv6

Contents

BFD commands

Basic BFD commands

bfd authentication-mode

Use **bfd authentication-mode** to configure the BFD authentication mode for single-hop BFD control packets.

Use **undo bfd authentication-mode** to restore the default.

Syntax

bfd authentication-mode { **hmac-md5** | **hmac-mmd5** | **hmac-msha1** | **hmac-sha1** | **m-md5** | **m-sha1** | **md5** | **sha1** | **simple** } *key-id* { **cipher** | **plain** } *string*

undo bfd authentication-mode

Default

Single-hop BFD control packets are not authenticated.

Views

Interface view

BFD template view

Predefined user roles

network-admin

Parameters

hmac-md5: Specifies the HMAC MD5 algorithm.

hmac-mmd5: Specifies the HMAC Meticulous MD5 algorithm.

hmac-msha1: Specifies the HMAC Meticulous SHA1 algorithm.

hmac-sha1: Specifies the HMAC SHA1 algorithm.

m-md5: Specifies the Meticulous MD5 algorithm.

m-sha1: Specifies the Meticulous SHA1 algorithm.

md5: Specifies the MD5 algorithm.

sha1: Specifies the SHA1 algorithm.

simple: Specifies the simple authentication mode.

key-id: Sets the authentication key ID in the range of 1 to 255.

cipher: Specifies a key in encrypted form.

plain: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. Its plaintext form is a case-sensitive string of 1 to 16 characters. Its encrypted form is a case-sensitive string of 33 to 53 characters.

Usage guidelines

Use this command to enhance BFD session security.

BFD version 0 does not support this command. The configuration does not take effect.

Examples

Configure VLAN-interface 11 to perform simple authentication for single-hop BFD control packets, setting the authentication key ID to **1** and plaintext key to **123456**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] bfd authentication-mode simple 1 plain 123456
```

bfd demand enable

Use **bfd demand enable** to enable the Demand BFD session mode.

Use **undo bfd demand enable** to restore the default.

Syntax

bfd demand enable

undo bfd demand enable

Default

The BFD session is in Asynchronous mode.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

In Demand mode, the device periodically sends BFD control packets. If the peer end is operating in Asynchronous mode (default), the peer end stops sending BFD control packets. If the peer end is operating in Demand mode, both ends stop sending BFD control packets. When the connectivity to another system needs to be verified explicitly, a system sends several BFD control packets with the Poll (P) bit set at the negotiated transmit interval. If no response is received within the detection interval, the session is considered down. If the connectivity is found to be up, no more BFD control packets are sent until the next command is issued.

In Asynchronous mode, the device periodically sends BFD control packets. The device considers that the session is down if it does not receive any BFD control packets within a specific interval.

BFD version 0 does not support this command. The configuration does not take effect.

Examples

Enable the Demand BFD session mode on VLAN-interface 11.

```
<Sysname> system-view
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] bfd demand enable
```

bfd detect-interface

Use **bfd detect-interface source-ip** to create a BFD session for detecting the local interface state.

Use **undo bfd detect-interface** to remove the BFD session.

Syntax

bfd detect-interface source-ip *ip-address* [**discriminator local** *local-value* **remote** *remote-value*] [**template** *template-name*]

undo bfd detect-interface

Default

No BFD session is created for detecting the local interface state.

Views

Interface view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the source IP address for BFD control packets.

discriminator: Specifies BFD session discriminators. If you do not specify discriminators, the device obtains BFD session discriminators through autonegotiation.

local *local-value*: Specifies the local discriminator. The value range for the *local-value* argument is 97 to 128.

remote *remote-value*: Specifies the remote discriminator in the range of 1 to 4294967295.

template *template-name*: Specifies a template by its name, a case-sensitive string of 1 to 63 characters. If you do not specify a template, the BFD session uses the BFD parameters configured in interface view.

Usage guidelines

This command implements fast collaboration between interface state and BFD session state. When BFD detects a link fault, it sets the link layer protocol state to DOWN(BFD). This behavior helps applications relying on the link layer protocol state achieve fast convergence.

The source IP address of control packets is specified manually, and the destination IP address is fixed at 224.0.0.184. As a best practice, specify the IP address of the interface as the source IP address. If the interface does not have an IP address, specify a unicast IP address other than 0.0.0.0 as the source IP address.

You can associate the state of the following interfaces with BFD:

- Layer 2 Ethernet interfaces.
- Member ports in a Layer 2 aggregation group.
- VLAN interfaces.
- Layer 2 aggregate interfaces.

This command must be executed on both ends of the link for a BFD session to be established.

If you execute both the **bfd detect-interface** and **bfd echo enable** commands for an interface, only the **bfd detect-interface** command takes effect.

For BFD detection to take effect, do not execute this command on both a Layer 2 Ethernet interface and the VLAN interface created for the VLAN to which the Layer 2 Ethernet interface is assigned.

For BFD detection to take effect, do not execute this command on the following interfaces at the same time:

- A Layer 2 aggregate interface.
- A member port of the Layer 2 aggregate interface.
- The VLAN interface to which the Layer 2 aggregate interface belongs.

If the peer device does not support obtaining BFD session discriminators through autonegotiation, you must specify the discriminators on both the local and peer devices. Without the discriminators, the BFD session cannot come up.

The BFD session discriminators must match on the local and peer devices. For example, if you configure **bfd detect-interface source-ip** 20.1.1.1 **discriminator local** 513 **remote** 514 on the local device, you must configure **bfd detect-interface source-ip** 20.1.1.2 **discriminator local** 514 **remote** 513 on the peer device.

The local discriminators of BFD sessions for interfaces on the same device must be different.

Examples

Create a BFD session to detect the state of VLAN-interface 10, and specify the source IP address as 20.1.1.1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] bfd detect-interface source-ip 20.1.1.1
```

bfd detect-interface first-fail-timer

Use **bfd detect-interface first-fail-timer** to configure the timer that delays reporting the first BFD session establishment failure to the data link layer.

Use **undo bfd detect-interface first-fail-timer** to restore the default.

Syntax

bfd detect-interface first-fail-timer *seconds*

undo bfd detect-interface first-fail-timer

Default

The first BFD session establishment failure is not reported to the data link layer.

Views

Interface view

Predefined user roles

network-admin

Parameters

seconds: Specifies the timeout time that reports the first BFD session establishment failure to the data link layer. The value range for this argument is 1 to 10000 seconds.

Usage guidelines

If the BFD session fails to be established when the timer expires, BFD reports the failure to the data link layer and sets the data link layer state of the interface to DOWN(BFD). This behavior rapidly identifies the interfaces for which BFD sessions fail to be established. In this case, the BFD session state is displayed as Down in the **display bfd session** command output. The line protocol state of the interface is displayed as DOWN(BFD) in the **display interface** command output.

If the local end is configured with the **bfd detect-interface** command, the BFD session for detecting the local interface state fails to be established when the following conditions exist:

- The remote end is not configured with the **bfd detect-interface** command.
- The local and remote ends have mismatching BFD authentication settings.

Examples

Configure the timer that delays reporting the first BFD session establishment failure as 10 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] bfd detect-interface first-fail-timer 10
```

Related commands

bfd detect-interface

display interface (*Interface Command Reference*)

bfd detect-interface special-processing

Use **bfd detect-interface special-processing** to enable special processing for BFD sessions.

Use **undo bfd detect-interface special-processing** to disable special processing for BFD sessions.

Syntax

bfd detect-interface special-processing [**admin-down** | **authentication-change** | **session-up**] *

undo bfd detect-interface special-processing [**admin-down** | **authentication-change** | **session-up**] *

Default

All types of special processing for BFD sessions are disabled.

Views

Interface view

Predefined user roles

network-admin

Parameters

admin-down: Notifies a session down event to the data link layer upon receipt of a BFD packet with the State field as AdminDown. This keyword helps rapidly discover interfaces that BFD sessions are manually shut down. If you do not specify this keyword, the device sets the BFD session state to Down, but does not notify the session down event to the data link layer.

authentication-change: Immediately sets the session to down state upon a local authentication information change. This keyword helps rapidly discover interfaces with authentication information changes. If you do not specify this keyword, the device sets the session to down state if authentication information inconsistency still persists after a period of time.

session-up: Ignores authentication information inconsistency when the local session is up. If there is a large number of BFD sessions, examining authentication information consistency affects device performance. If you do not specify this keyword, the device examines authentication information in incoming BFD packets when the local session state is up. If the authentication information does not match on the two ends, the BFD session is declared down.

Usage guidelines

If you do not specify any parameters, this command enables or disables all types of special processing.

Examples

Enable all types of special processing for BFD sessions on VLAN-interface 11.

```
<Sysname> system-view
[Sysname] interface vlan-interface 11
```

```
[Sysname-Vlan-interface11] bfd detect-interface special-processing admin-down
authentication-change session-up
```

bfd detect-multiplier

Use **bfd detect-multiplier** to set the single-hop detection time multiplier for control packet mode and the detection time multiplier for echo packet mode.

Use **undo bfd detect-multiplier** to restore the default.

Syntax

bfd detect-multiplier *value*

undo bfd detect-multiplier

Default

The single-hop detection time multiplier for control packet mode and the detection time multiplier for echo packet mode are both 5.

Views

Interface view

BFD template view

Predefined user roles

network-admin

Parameters

value: Specifies a detection time multiplier. The value range for this argument is 3 to 50.

Usage guidelines

The detection time multiplier determines the maximum number of concurrent BFD packets (including control packets and echo packets) that can be discarded.

Table 1 Actual detection interval calculation method

Mode	Actual detection interval of the sender
Echo packet mode	Detection time multiplier of the sender × actual packet sending interval of the sender
Control packet mode BFD session in asynchronous mode	Detection time multiplier of the receiver × MAX (minimum receiving interval supported by the sender, minimum sending interval supported by the receiver)
Control packet mode BFD session in demand mode	Detection time multiplier of the sender × MAX (minimum sending interval supported by the sender, minimum receiving interval supported by the receiver)

Examples

Set the single-hop detection time multiplier for control packet mode and the detection time multiplier for echo packet mode to 6 on VLAN-interface 11.

```
<Sysname> system-view
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] bfd detect-multiplier 6
```

bfd echo enable

Use **bfd echo enable** to enable the echo packet mode.

Use **undo bfd echo enable** to disable the echo packet mode.

Syntax

bfd echo [**receive** | **send**] **enable**

undo bfd echo [**receive** | **send**] **enable**

Default

The echo packet mode is disabled.

Views

Interface view

Predefined user roles

network-admin

Parameters

receive: Specifies the echo packet receiving capability.

send: Specifies the echo packet sending capability.

Usage guidelines

If you enable the echo packet mode for a BFD session in which control packets are sent and the session comes up, BFD performs the following operations:

- Periodically sends echo packets to detect link connectivity.
- Decreases the control packet receiving rate at the same time.

To enable only the echo packet receiving capability, use the **bfd echo receive enable** command.

To enable only the echo packet sending capability, use the **bfd echo send enable** command.

If you do not specify the **receive** or **send** keyword, the command enables both the echo packet receiving and sending capabilities.

If you configure both the **bfd detect-interface** and **bfd echo enable** commands for an interface, only the **bfd detect-interface** command takes effect.

BFD version 0 does not support this command. The configuration does not take effect.

Examples

Enable the echo packet mode on VLAN-interface 11.

```
<Sysname> system-view
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] bfd echo enable
```

bfd echo-source-ip

Use **bfd echo-source-ip** to configure the source IP address of BFD echo packets.

Use **undo bfd echo-source-ip** to remove the configured source IP address of BFD echo packets.

Syntax

bfd echo-source-ip *ip-address*

undo bfd echo-source-ip

Default

No source IP address is configured for BFD echo packets.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the source IP address of BFD echo packets.

Usage guidelines

The source IP address cannot be on the same network segment as any local interface's IP address. Otherwise, a large number of ICMP redirect packets might be sent from the peer, resulting in link congestion.

Examples

Configure the source IP address of BFD echo packets as 8.8.8.8.

```
<Sysname> system-view
[Sysname] bfd echo-source-ip 8.8.8.8
```

bfd echo-source-ipv6

Use **bfd echo-source-ipv6** to configure the source IPv6 address of BFD echo packets.

Use **undo bfd echo-source-ipv6** to remove the configured source IPv6 address of BFD echo packets.

Syntax

bfd echo-source-ipv6 *ipv6-address*

undo bfd echo-source-ipv6

Default

No source IPv6 address is configured for BFD echo packets.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the source IPv6 address for BFD echo packets.

Usage guidelines

The source IPv6 address of echo packets can only be a global unicast address.

The source IPv6 address cannot be on the same network segment as any local interface's IP address. Otherwise, a large number of ICMP redirect packets might be sent from the peer, resulting in link congestion.

Examples

Configure the source IPv6 address of BFD echo packets as 80::2.

```
<Sysname> system-view
[Sysname] bfd echo-source-ipv6 80::2
```

bfd min-echo-receive-interval

Use **bfd min-echo-receive-interval** to set the minimum interval for receiving BFD echo packets.

Use **undo bfd min-echo-receive-interval** to restore the default.

Syntax

bfd min-echo-receive-interval *interval*

undo bfd min-echo-receive-interval

Default

The minimum interval for receiving BFD echo packets is 400 milliseconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

interval: Specifies the minimum interval for receiving BFD echo packets, in milliseconds. The value takes 0 or is in the range of 100 to 1000.

Usage guidelines

This command sets the BFD echo packet receiving interval, which is the actual BFD echo packet sending interval.

The local end stops sending echo packets after autonegotiation with the remote end if the following conditions are met:

- The echo packet mode is enabled on the local end.
- The minimum interval for receiving BFD echo packets is set to 0 milliseconds on the remote end.

Examples

Set the minimum interval for receiving BFD echo packets to 500 milliseconds on VLAN-interface 11.

```
<Sysname> system-view
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] bfd min-echo-receive-interval 500
```

bfd min-receive-interval

Use **bfd min-receive-interval** to set the minimum interval for receiving single-hop BFD control packets.

Use **undo bfd min-receive-interval** to restore the default.

Syntax

bfd min-receive-interval *interval*

undo bfd min-receive-interval

Default

The minimum interval for receiving single-hop BFD control packets is 400 milliseconds.

Views

Interface view

BFD template view

Predefined user roles

network-admin

Parameters

interval: Specifies the minimum interval for receiving single-hop BFD control packets, in milliseconds. The value range is 100 to 1000.

Usage guidelines

Use this command to prevent the control packet sending rate of the peer end from exceeding the control packet receiving rate of the local end.

The actual control packet sending interval of the peer end takes the greater value between the following values:

- Minimum interval for transmitting BFD control packets on the peer end.
- Minimum interval for receiving BFD control packets on the local end.

Examples

Set the minimum interval for receiving single-hop BFD control packets to 500 milliseconds on VLAN-interface 11.

```
<Sysname> system-view
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] bfd min-receive-interval 500
```

bfd min-transmit-interval

Use **bfd min-transmit-interval** to set the minimum interval for transmitting single-hop BFD control packets.

Use **undo bfd min-transmit-interval** to restore the default.

Syntax

bfd min-transmit-interval *interval*

undo bfd min-transmit-interval

Default

The minimum interval for transmitting single-hop BFD control packets is 400 milliseconds.

Views

Interface view

BFD template view

Predefined user roles

network-admin

Parameters

interval: Specifies the minimum interval for transmitting single-hop BFD control packets, in milliseconds. The value range is 100 to 1000.

Usage guidelines

Use this command to prevent the BFD packet sending rate from exceeding the device capability.

The actual BFD control packet transmitting interval on the local end is the greater value between the following values:

- Minimum interval for transmitting BFD control packets on the local end.
- Minimum interval for receiving BFD control packets on the peer end.

Examples

Set the minimum interval for transmitting single-hop BFD control packets to 500 milliseconds on VLAN-interface 11.

```
<Sysname> system-view
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] bfd min-transmit-interval 500
```

bfd multi-hop authentication-mode

Use **bfd multi-hop authentication-mode** to configure the authentication mode for multihop BFD control packets.

Use **undo bfd multi-hop authentication-mode** to restore the default.

Syntax

bfd multi-hop authentication-mode { **hmac-md5** | **hmac-mmd5** | **hmac-msha1** | **hmac-sha1** | **m-md5** | **m-sha1** | **md5** | **sha1** | **simple** } *key-id* { **cipher** | **plain** } *string*

undo bfd multi-hop authentication-mode

Default

No authentication is performed.

Views

System view

Predefined user roles

network-admin

Parameters

hmac-md5: Specifies the HMAC MD5 algorithm.

hmac-mmd5: Specifies the HMAC Meticulous MD5 algorithm.

hmac-msha1: Specifies the HMAC Meticulous SHA1 algorithm.

hmac-sha1: Specifies the HMAC SHA1 algorithm.

m-md5: Specifies the Meticulous MD5 algorithm.

m-sha1: Specifies the Meticulous SHA1 algorithm.

md5: Specifies the MD5 algorithm.

sha1: Specifies the SHA1 algorithm.

simple: Specifies the simple authentication mode.

key-id: Sets the authentication key ID in the range of 1 to 255.

cipher: Specifies a key in encrypted form.

plain: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. Its plaintext form is a case-sensitive string of 1 to 16 characters. Its encrypted form is a case-sensitive string of 33 to 53 characters.

Usage guidelines

Use this command to enhance BFD session security.

BFD version 0 does not support this command. The configuration does not take effect.

Examples

Configure the simple authentication mode for multihop BFD control packets, setting the authentication key ID to 1 and key to **123456**.

```
<Sysname> system-view
[Sysname] bfd multi-hop authentication-mode simple 1 plain 123456
```

bfd multi-hop destination-port

Use **bfd multi-hop destination-port** to configure the destination port number for multihop BFD control packets.

Use **undo bfd multi-hop destination-port** to restore the default.

Syntax

bfd multi-hop destination-port *port-number*

undo bfd multi-hop destination-port

Default

The destination port number for multihop BFD control packets is 4784.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies the destination port number of multihop BFD control packets, 3784 or 4784.

Examples

Specify the destination port number for multihop BFD control packets as 3784.

```
<Sysname> system-view
[Sysname] bfd multi-hop destination-port 3784
```

bfd multi-hop detect-multiplier

Use **bfd multi-hop detect-multiplier** to set the multihop detection time multiplier for control packet mode.

Use **undo bfd multi-hop detect-multiplier** to restore the default.

Syntax

bfd multi-hop detect-multiplier *value*

undo bfd multi-hop detect-multiplier

Default

The multihop detection time multiplier for control packet mode is 5.

Views

System view

Predefined user roles

network-admin

Parameters

value: Specifies the multihop detection time multiplier in the range of 3 to 50.

Usage guidelines

The detection time multiplier determines the maximum number of concurrent BFD control packets that can be discarded.

Table 2 Actual detection interval calculation method

Mode	Actual detection interval of the sender
Control packet mode BFD session in asynchronous mode	Detection time multiplier of the receiver × MAX (minimum receiving interval supported by the sender, minimum sending interval supported by the receiver)
Control packet mode BFD session in demand mode	Detection time multiplier of the sender × MAX (minimum sending interval supported by the sender, minimum receiving interval supported by the receiver)

Examples

Set the multihop detection time multiplier to 6.

```
<Sysname> system-view
[Sysname] bfd multi-hop detect-multiplier 6
```

bfd multi-hop min-receive-interval

Use **bfd multi-hop min-receive-interval** to set the minimum interval for receiving multihop BFD control packets.

Use **undo bfd multi-hop min-receive-interval** to restore the default.

Syntax

bfd multi-hop min-receive-interval *interval*

undo bfd multi-hop min-receive-interval

Default

The minimum interval for receiving multihop BFD control packets is 400 milliseconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the minimum interval for receiving multihop BFD control packets, in milliseconds. The value range is 100 to 1000.

Usage guidelines

Use this command to prevent the packet sending rate of the peer end from exceeding the packet receiving capability (minimum control packet receiving interval) of the local end. If the receiving capability is exceeded, the peer end dynamically adjusts the BFD control packet sending interval to the minimum control packet receiving interval of the local end.

Examples

Set the minimum interval for receiving multihop BFD control packets to 500 milliseconds.

```
<Sysname> system-view
[Sysname] bfd multi-hop min-receive-interval 500
```

bfd multi-hop min-transmit-interval

Use **bfd multi-hop min-transmit-interval** to set the minimum interval for transmitting multihop BFD control packets.

Use **undo bfd multi-hop min-transmit-interval** to restore the default.

Syntax

bfd multi-hop min-transmit-interval *interval*

undo bfd multi-hop min-transmit-interval

Default

The minimum interval for transmitting multihop BFD control packets is 400 milliseconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the minimum interval for transmitting multihop BFD control packets, in milliseconds. The value range is 100 to 1000.

Usage guidelines

Use this command to prevent the BFD packet sending rate from exceeding the device capability.

The actual BFD control packet transmitting interval on the local end is the greater value between the following values:

- Minimum interval for transmitting BFD control packets on the local end.
- Minimum interval for receiving BFD control packets on the peer end.

Examples

Set the minimum interval for transmitting multihop BFD control packets to 500 milliseconds.

```
<Sysname> system-view
[Sysname] bfd multi-hop min-transmit-interval 500
```

bfd session init-mode

Use **bfd session init-mode** to configure the mode for establishing a BFD session.

Use **undo bfd session init-mode** to restore the default.

Syntax

bfd session init-mode { **active** | **passive** }

undo bfd session init-mode

Default

BFD uses the **active** mode.

Views

System view

Predefined user roles

network-admin

Parameters

active: Specifies the active mode. In active mode, BFD actively transmits BFD control packets to the remote device, regardless of whether it receives a BFD control packet from the remote device.

passive: Specifies the passive mode. In passive mode, BFD does not actively transmit a BFD control packet to the remote end; it transmits a BFD control packet only after receiving a BFD control packet from the remote end.

Usage guidelines

A minimum of one end must operate in active mode for a BFD session to be established.

BFD version 0 does not support this command. The configuration does not take effect.

Examples

Configure the session establishment mode as **passive**.

```
<Sysname> system-view
[Sysname] bfd session init-mode passive
```

bfd template

Use **bfd template** to create a BFD template and enter its view, or enter the view of an existing BFD template.

Use **undo bfd template** to delete the BFD template.

Syntax

bfd template *template-name*

undo bfd template *template-name*

Default

No BFD templates exist.

Views

System view

Predefined user roles

network-admin

Parameters

template-name: Specifies the template name, a case-sensitive string of 1 to 63 characters.

Examples

Create BFD template **bfd1** and enter BFD template view.

```
<Sysname> system-view
[Sysname] bfd template bfd1
[Sysname-bfd-template-bfd1]
```

display bfd session

Use **display bfd session** to display BFD session information.

Syntax

display bfd session [**discriminator** *value* | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

discriminator *value*: Specifies a local ID in the range of 1 to 4294967295. If this option is not specified, the command displays brief information about all BFD sessions.

verbose: Displays detailed BFD session information. If this keyword is not specified, the command displays brief BFD session information.

Examples

Display brief information about all IPv4 BFD sessions.

```
<Sysname> display bfd session

 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv4 session working in control packet mode:

 LD/RD          SourceAddr      DestAddr        State    Holdtime    Interface
 513/513        1.1.1.1         1.1.1.2         Up       2297ms      Vlan100
```

Display detailed IPv4 BFD session information.

```
<Sysname> display bfd session verbose

 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv4 session working in control packet mode:

      Local Discr: 513                Remote Discr: 513
        Source IP: 1.1.1.1           Destination IP: 1.1.1.2
    Session State: Up                     Interface: Vlan-interface100
     Min Tx Inter: 500ms                Act Tx Inter: 500ms
```

```
      Min Rx Inter: 500ms               Detect Inter: 2500ms
          Rx Count: 42                      Tx Count: 43
      Connect Type: Direct             Running Up for: 00:00:20
         Hold Time: 2078ms                 Auth mode: None
       Detect Mode: Async                       Slot: 0
          Protocol: OSPF
          Version:1
         Diag Info: No Diagnostic
```

Display brief information about all IPv6 BFD sessions.

```
<Sysname> display bfd session

 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv6 session working in control packet mode:

       Local Discr: 513                 Remote Discr: 513
         Source IP: FE80::20C:29FF:FED4:7171
    Destination IP: FE80::20C:29FF:FE72:AC4D
     Session State: Up                     Interface: Vlan100
         Hold Time: 2142ms
```

Display detailed IPv6 BFD session information.

```
<Sysname> display bfd session verbose

 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv6 session working in control packet mode:

       Local Discr: 513                 Remote Discr: 513
         Source IP: FE80::20C:29FF:FED4:7171
    Destination IP: FE80::20C:29FF:FE72:AC4D
     Session State: Up                     Interface: Vlan-interface100
      Min Tx Inter: 500ms               Act Tx Inter: 500ms
      Min Rx Inter: 500ms               Detect Inter: 2500ms
          Rx Count: 38                      Tx Count: 38
      Connect Type: Direct             Running Up for: 00:00:15
         Hold Time: 2211ms                 Auth mode: None
       Detect Mode: Async                       Slot: 0
          Protocol: OSPFv3
          Version:1
         Diag Info: No Diagnostic
```

Table 3 Command output

Field	Description
Total Session Num	Total number of BFD sessions.
Up Session Num	Total number of active BFD sessions.
Init Mode	BFD operating mode: Active or passive.

Field	Description
IPv4 session working in control packet mode	BFD session type and operating mode: • **IPv4 session working in control packet mode**. • **IPv4 session working in echo mode**. • **IPv6 session working in control packet mode**. • **IPv6 session working in echo mode**.
Local Discr/LD	Local discriminator of the session.
Remote Discr/RD	Remote discriminator of the session.
Source IP/SourceAddr	Source IP address of the session.
Destination IP/DestAddr	Destination IP address of the session.
Session State/State	Session state: **Down**, **Init**, or **Up**.
Interface	Name of the interface of the session.
Min Tx Inter	Minimum BFD packet transmission interval.
Min Rx Inter	Minimum BFD packet receiving interval.
Act Tx Inter	Actual BFD packet transmission interval.
Detect Inter	Actual session detection timer.
Rx Count	Number of packets received.
Tx Count	Number of packets sent.
Hold Time/Holdtime	Length of time before the session detection timer expires, in milliseconds. For a BFD session in **Down** state, this field displays **0ms**.
Auth mode	Session authentication mode.
Connect Type	Connection type of the interface: Direct or indirect.
Running up for	Time period for which the session has been up.
Detect Mode	Detection mode: • **Async**—Asynchronous mode. • **Demand**—Demand mode. • **Async/Echo**—Asynchronous mode with echo detection enabled. • **Demand/Echo**—Demand mode with echo detection enabled.
Slot	Slot number.
Diag Info	Diagnostic information about the session: • **No Diagnostic**. • **Control Detection Time Expired**—A control packet mode BFD session goes down because local detection times out. • **Echo Function Failed**—An echo packet mode BFD session goes down, because local detection times out or the source IP address of echo packets is deleted. • **Neighbor Signaled Session Down**—The remote end notifies the local end of BFD session down. • **Administratively Down**—The local system prevents a BFD session from being established.

reset bfd session statistics

Use **reset bfd session statistics** to clear the BFD session statistics.

Syntax

reset bfd session statistics

Views

User view

Predefined user roles

network-admin

Examples

Clear the BFD session statistics.

```
<Sysname> reset bfd session statistics
```

snmp-agent trap enable bfd

Use **snmp-agent trap enable bfd** to enable SNMP notifications for BFD.

Use **undo snmp-agent trap enable bfd** to disable SNMP notifications for BFD.

Syntax

snmp-agent trap enable bfd

undo snmp-agent trap enable bfd

Default

All SNMP notifications are enabled for BFD.

Views

System view

Predefined user roles

network-admin

Usage guidelines

To report critical BFD events to an NMS, enable SNMP notifications for BFD. For BFD event notifications to be sent correctly, you must also configure SNMP as described in the network management and monitoring configuration guide for the device.

Examples

Disable SNMP notifications for BFD.

```
<Sysname> system-view
[Sysname] undo snmp-agent trap enable bfd
```

Contents

Track commands

delay

Use **delay** to set the period of time that the Track module must wait before notifying the application module of track entry state changes.

Use **undo delay** to remove the notification delay configuration.

Syntax

delay { **negative** *negative-time* | **positive** *positive-time* } *

undo delay

Default

The Track module notifies the application module immediately when the track entry state changes.

Views

Track view

Predefined user roles

network-admin

Parameters

negative *negative-time*: Specifies the delay for notifying the application module that the track entry state has changed to Negative. The *negative-time* argument represents the negative state notification delay in the range of 1 to 300 seconds.

positive *positive-time*: Specifies the delay for notifying the application module that the track entry state has changed to Positive. The *positive-time* argument represents the positive state notification delay in the range of 1 to 300 seconds.

Usage guidelines

If the Track module immediately notifies the application module of a track entry state change but route convergence is not complete, a communication failure might occur. To address this issue, you can set a notification delay to avoid immediate notification of track entry state changes.

The notification delay settings do not take effect if the track entry is not associated with an application module.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the negative state notification delay to 50 seconds and the positive state notification delay to 120 seconds for track entry 101 associated with a Boolean OR list.

```
<Sysname> system-view
[Sysname] track 101 list boolean or
[Sysname-track-101] delay negative 50 positive 120
```

Related commands

track bfd

track cfd

track interface

track ip route reachability

track list boolean

track list threshold percentage

track list threshold weight

track nqa

display track

Use **display track** to display track entry information.

Syntax

display track { *track-entry-number* | **all** [**negative** | **positive**] } [**brief**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

track-entry-number: Specifies the track entry ID in the range of 1 to 1024.

all: Specifies all track entries.

negative: Specifies track entries in Negative state.

positive: Specifies track entries in Positive state.

brief: Displays brief information about track entries.

Examples

Display information about all track entries.

```
<Sysname> display track all
Track ID: 1
  State: Positive
  Duration: 0 days 0 hours 0 minutes 7 seconds
  Tracked object type: NQA
  Notification delay: Positive 20, Negative 30 (in seconds)
  Tracked object:
    NQA entry: admin test
    Reaction: 10
    Remote IP/URL: 2.2.2.2
    Local IP: 1.1.1.1
    Interface: Vlan-interface1
Track ID: 2
  State: NotReady
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Tracked object type: BFD ctrl
  Notification delay: Positive 20, Negative 30 (in seconds)
  Tracked object:
    BFD session mode: Echo
    Outgoing interface: Vlan-interface2
```

```
    VPN instance name: --
    Remote IP: 192.168.40.1
    Local IP: 192.168.40.2
Track ID: 3
  State: Negative
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Tracked object type: Interface
  Notification delay: Positive 20, Negative 30 (in seconds)
  Tracked object:
    Interface:  Vlan-interface3
    Protocol: IPv4
Track ID: 4
  State: Negative
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Tracked object type: CFD
  Notification delay: Positive 20, Negative 30 (in seconds)
  Tracked object:
    CFD service instance: MEP 2 in Ethernet service instance 1
Track ID: 6
  State: Positive
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Tracked object type: Failover group
  Notification delay: Positive 20, Negative 30 (in seconds)
  Tracked object:
    LLDP interface: Vlan-interface4
```

Display information about track entries in Negative state.

```
<Sysname> display track all negative brief
ID   Status   Type      Remote IP/URL   Local IP        Interface
1    Negative Interface --              --              Vlan2
10   Negative Interface --              --              Vlan3
```

Table 1 Command output

Field	Description
Track ID	ID of a track entry.
State	States of a track entry: • **Positive**—The tracked object operates correctly. • **NotReady**—The tracked object is invalid. • **Negative**—The tracked object is abnormal.
Duration	Time period during which the track entry stays in the state.

Field	Description
Type	Tracked object type: • **BFD ctrl**—Control-mode BFD session. • **BFD echo**—Echo-mode BFD session. • **CFD**. • **Interface**. • **Route**. • **NQA**. • **LLDP**. This field is displayed only when the **`display track brief`** command is executed.
Tracked object type	Tracked object type: • **BFD ctrl**—Control-mode BFD session. • **BFD echo**—Echo-mode BFD session. • **CFD echo**. • **Interface**. • **Route**. • **LLDP**. • **NQA**.
Notification delay: Positive 20, Negative 30 (in seconds)	• The Track module notifies the application modules that the status of the track entry changes to Positive after a delay time of 20 seconds. • The Track module notifies the application modules that the status of the track entry changes to Negative after a delay time of 30 seconds.
Tracked object	Tracked object associated with the track entry.
NQA entry	NQA operation associated with the track entry.
Reaction	Reaction entry associated with the track entry.
BFD session mode	BFD session mode.
Outgoing interface	Outgoing interface of BFD echo packets.
VPN instance name	This field is not supported in the current software version. Name of the VPN instance to which BFD session packets belong. If the packets belong to the public network, two consecutive hyphens (--) are displayed.
Remote IP/URL	Remote IP address or URL. If no remote IP address or URL exists, two consecutive hyphens (--) are displayed.
Local IP	Local IP address. If no local IP address exists, two consecutive hyphens (--) are displayed.
Interface	Interface to be monitored. If no interface is to be monitored, two consecutive hyphens (--) are displayed.
Protocol	Link states or Layer 3 protocol states of the monitored interface: • **None**—Link status of the monitored interface. • **IPv4**—IPv4 protocol status of the monitored Layer 3 interface. • **IPv6**—IPv6 protocol status of the monitored Layer 3 interface.
IP route	Route associated with the track entry.

Field	Description
VPN instance name	This field is not supported in the current software version. Name of the VPN instance to which the route belongs. If the route belongs to the public network, two consecutive hyphens (--) are displayed.
Protocol	Protocol type of the route. If the route does not exist, **N/A** is displayed.
Nexthop interface	Next hop of the route. If the route does not exist, **N/A** is displayed.
LLDP interface	Monitored LLDP interface.

Related commands

track bfd ctrl

track bfd echo

track cfd

track interface

track interface physical

track interface protocol

track ip route reachability

track lldp neighbor

track nqa

track bfd ctrl

Use **track bfd ctrl** to create a track entry associated with a control-mode BFD session and enter Track view, or enter the view of an existing track entry.

Use **undo track** to remove the track entry and all its settings.

Syntax

track *track-entry-number* **bfd ctrl** [**interface** *interface-type interface-number*] **remote ip** *remote-ip-address* **local ip** *local-ip-address*

undo track *track-entry-number*

Default

No track entries exist.

Views

System view

Predefined user roles

network-admin

Parameters

track-entry-number: Specifies the track entry ID in the range of 1 to 1024.

interface *interface-type interface-number*: Specifies the outgoing interface by its type and number of BFD control packets. If you do not specify an outgoing interface, the outgoing interface found through FIB table lookup is used.

remote ip *remote-ip-address*: Specifies the destination IP address of the BFD control packets. The specified IP address must be the IP address of a directly connected interface.

local ip *local-ip-address*: Specifies the source IP address of the BFD control packets. The specified IP address must be the IP address of a directly connected interface.

Usage guidelines

To create a track entry, you must specify the tracked object type, which is **bfd ctrl** in this command.

To enter the view of an existing track entry, use the **track** *track-entry-number* command. The tracked object type is not required.

To modify the settings of a track entry, execute the **undo track** command to remove the track entry, and then execute the **track bfd ctrl** command again.

When you associate Track with a BFD session, do not use the virtual IP address of a VRRP group as the local or remote IP address of the BFD session.

Examples

Associate track entry 1 with a control-mode BFD session. The BFD control packets use destination IP address 192.168.1.1, source IP address 192.168.1.2, and outgoing interface VLAN-interface 2.

```
<Sysname> system-view
[Sysname] track 1 bfd ctrl interface vlan-interface 2 remote ip 192.168.1.1 local ip
192.168.1.2
[Sysname-track-1]
```

Related commands

delay

display track

track bfd echo

Use **track bfd echo** to create a track entry associated with an echo-mode BFD session and enter Track view, or enter the view of an existing track entry.

Use **undo track** to remove the track entry and all its settings.

Syntax

track *track-entry-number* **bfd echo interface** *interface-type interface-number* **remote ip** *remote-ip-address* **local ip** *local-ip-address*

undo track *track-entry-number*

Default

No track entries exist.

Views

System view

Predefined user roles

network-admin

Parameters

track-entry-number: Specifies the track entry ID in the range of 1 to 1024.

interface *interface-type interface-number*: Specifies the outgoing interface by its type and number of the BFD echo packets.

remote ip *remote-ip-address*: Specifies the destination IP address of the BFD echo packets. The specified IP address must be the IP address of a directly connected interface.

local ip *local-ip-address*: Specifies the source IP address of the BFD echo packets. The specified IP address must be the IP address of a directly connected interface.

Usage guidelines

To create a track entry, you must specify the tracked object type, which is **bfd echo** in this command.

To enter the view of an existing track entry, use the **track** *track-entry-number* command. The tracked object type is not required.

To modify the settings of a track entry, execute the **undo track** command to remove the track entry, and then execute the **track bfd echo** command again.

When you associate Track with BFD, the virtual IP address of a VRRP group cannot be the local or remote address of a BFD session.

Examples

Associate track entry 1 with an echo-mode BFD session. The BFD echo packets use destination IP address 1.1.1.1, source IP address 1.1.1.2, and outgoing interface VLAN-interface 2.

```
<Sysname> system-view
[Sysname] track 1 bfd echo interface vlan-interface 2 remote ip 1.1.1.1 local ip 1.1.1.2
[Sysname-track-1]
```

Related commands

delay

display track

track cfd

Use **track cfd** to create a track entry associated with CFD and enter Track view, or enter the view of an existing track entry.

Use **undo track** to remove the track entry and all its settings.

Syntax

track *track-entry-number* **cfd cc service-instance** *instance-id* **mep** *mep-id*

undo track *track-entry-number*

Default

No track entries exist.

Views

System view

Predefined user roles

network-admin

Parameters

track-entry-number: Specifies the track entry ID in the range of 1 to 1024.

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767.

mep *mep-id*: Specifies a MEP by its ID in the range of 1 to 8191.

Usage guidelines

To create a track entry, you must specify the tracked object type, which is **cfd** in this command.

To enter the view of an existing track entry, use the **track** *track-entry-number* command. The tracked object type is not required.

To modify the settings of a track entry, execute the **undo track** command to remove the track entry, and then execute the **track cfd** command again.

Examples

Create track entry 1 and specify the CFD service instance ID as 2 and MEP ID as 3.

```
<Sysname> system-view
[Sysname] track 1 cfd cc service-instance 2 mep 3
[Sysname-track-1]
```

Related commands

cfd mep

cfd service-instance

delay

display track

track interface

Use **track interface** to create a track entry associated with the link state of an interface and enter Track view, or enter the view of an existing track entry.

Use **undo track** to remove the track entry and all its settings.

Syntax

track *track-entry-number* **interface** *interface-type interface-number*

undo track *track-entry-number*

Default

No track entries exist.

Views

System view

Predefined user roles

network-admin

Parameters

track-entry-number: Specifies the track entry ID in the range of 1 to 1024.

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

To create a track entry, you must specify the tracked object type, which is **interface** in this command.

To enter the view of an existing track entry, use the **track** *track-entry-number* command. The tracked object type is not required.

When you associate Track with interface management to monitor the link status of an interface, the track entry state changes as follows:

- The track entry state is Positive if the link state of the interface is up.
- The track entry state is Negative if the link state of the interface is down.

To display the link state of an interface, use the **display ip interface brief** command.

To modify the settings of a track entry, execute the **undo track** command to remove the track entry, and then execute the **track interface** command again.

Examples

Create track entry 1 and associate it with the link state of interface VLAN-interface 10.

```
<Sysname> system-view
[Sysname] track 1 interface vlan-interface 10
[Sysname-track-1]
```

Related commands

delay

display ip interface brief (*Layer 3—IP Services Command Reference*)

display track

track interface physical

Use **track interface physical** to create a track entry associated with the physical state of an interface and enter Track view, or enter the view of an existing track entry.

Use **undo track** to remove the track entry and all its settings.

Syntax

track *track-entry-number* **interface** *interface-type interface-number* **physical**

undo track *track-entry-number*

Default

No track entries exist.

Views

System view

Predefined user roles

network-admin

Parameters

track-entry-number: Specifies the track entry ID in the range of 1 to 1024.

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

To create a track entry, you must specify the tracked object type, which is **interface physical** in this command.

To enter the view of an existing track entry, use the **track** *track-entry-number* command. The tracked object type is not required.

To modify the settings of a track entry, execute the **undo track** command to remove the track entry, and then execute the **track interface physical** command again.

Examples

Create track entry 1 and associate it with the physical state of VLAN-interface 2.

```
<Sysname> system-view
[Sysname] track 1 interface vlan-interface 2 physical
[Sysname-track-1]
```

Related commands

delay

display ip interface brief (*Layer 3—IP Services Command Reference*)

display track

track interface protocol

Use **track interface protocol** to create a track entry associated with the protocol state of an interface and enter Track view, or enter the view of an existing track entry.

Use **undo track** to remove the track entry and all its settings.

Syntax

track *track-entry-number* **interface** *interface-type interface-number* **protocol** { **ipv4** | **ipv6** }

undo track *track-entry-number*

Default

No track entries exist.

Views

System view

Predefined user roles

network-admin

Parameters

track-entry-number: Specifies the track entry ID in the range of 1 to 1024.

interface-type interface-number: Specifies an interface by its type and number.

ipv4: Monitors the IPv4 protocol state. When the IPv4 protocol state of an interface is up, the state of the track object is Positive. When the IPv4 protocol state of an interface is down, the state of the track object is Negative. To display the IPv4 protocol state of an interface, use the **display ip interface brief** command.

ipv6: Monitors the IPv6 protocol state. When the IPv6 protocol state of an interface is up, the state of the track object is Positive. When the IPv6 protocol state of an interface is down, the state of the track object is Negative. To display the IPv6 protocol state of an interface, use the **display ipv6 interface brief** command.

Usage guidelines

To create a track entry, you must specify the tracked object type, which is **interface protocol** in this command.

To enter the view of an existing track entry, use the **track** *track-entry-number* command. The tracked object type is not required.

To modify the settings of a track entry, execute the **undo track** command to remove the track entry, and then execute the **track interface protocol** command again.

Examples

Create track entry 1 and associate it with the IPv4 protocol state of interface VLAN-interface 2.

```
<Sysname> system-view
[Sysname] track 1 interface vlan-interface 2 protocol ipv4
[Sysname-track-1]
```

Related commands

delay

display ip interface brief (*Layer 3—IP Services Command Reference*)

display ipv6 interface brief (*Layer 3—IP Services Command Reference*)

display track

track ip route reachability

Use **track ip route reachability** to create a track entry associated with a route entry and enter Track view, or enter the view of an existing track entry.

Use **undo track** to remove the track entry and all its settings.

Syntax

track *track-entry-number* **ip route** *ip-address* { *mask-length* | *mask* } **reachability**

undo track *track-entry-number*

Default

No track entries exist.

Views

System view

Predefined user roles

network-admin

Parameters

track-entry-number: Specifies the track entry ID in the range of 1 to 1024.

ip-address: Specifies the IP address of the route entry associated with the track entry in dotted decimal notation.

mask-length: Specifies the mask length in the range of 0 to 32.

mask: Specifies the mask of the IP address, in dotted decimal notation.

Usage guidelines

To create a track entry, you must specify the tracked object type, which is **ip route reachability** in this command.

To enter the view of an existing track entry, use the **track** *track-entry-number* command. The tracked object type is not required.

To modify the settings of a track entry, execute the **undo track** command to remove the track entry, and then execute the **track ip route reachability** command again.

Route management does not immediately notify the Track module of the route status changes when the following conditions are met:

- An active/standby device switchover or a RIB process switchover has occurred.

- The status of the monitored route entry is changed before the routing protocol completes the graceful restart.

You can resolve the problem by configuring the nonstop routing feature.

Examples

Create track entry 1 to monitor the status of the route entry 10.1.1.0/24.

```
<Sysname> system-view
[Sysname] track 1 ip route 10.1.1.0 24 reachability
[Sysname-track-1]
```

Related commands

delay

display ip route (*Layer 3—IP Routing Command Reference*)

display track

track lldp neighbor

Use **track lldp neighbor** to create a track entry associated with the neighbor availability status of an LLDP interface and enter Track view, or enter the view of an existing track entry.

Use **undo track** to remove the track entry and all its settings.

Syntax

track *track-entry-number* **lldp neighbor interface** *interface-type interface-number*

undo track *track-entry-number*

Default

No track entries exist.

Views

System view

Predefined user roles

network-admin

Parameters

track-entry-number: Specifies the track entry ID in the range of 1 to 1024.

interface *interface-type interface-number*: Specifies an LLDP interface by its type and number.

Usage guidelines

To create a track entry, you must specify the tracked object type, which is **lldp neighbor** in this command.

To enter the view of an existing track entry, use the **track** *track-entry-number* command. The tracked object type is not required.

To modify the settings for a track entry, execute the **undo track** command to remove the track entry, and then execute the **track lldp neighbor** command again.

Examples

Create track entry 1 to monitor the neighbor availability status of GigabitEthernet 1/0/1.

```
<Sysname> system-view
```

```
[Sysname] track 1 lldp neighbor interface gigabitethernet 1/0/1
[Sysname-track-1]
```

Related commands

delay

display track

track nqa

Use **track nqa** to create a track entry associated with the reaction entry of an NQA operation and enter Track view, or enter the view of an existing track entry.

Use **undo track** to remove the track entry and all its settings.

Syntax

track *track-entry-number* **nqa entry** *admin-name operation-tag* **reaction** *item-number*

undo track *track-entry-number*

Default

No track entries exist.

Views

System view

Predefined user roles

network-admin

Parameters

track-entry-number: Specifies the track entry ID in the range of 1 to 1024.

entry *admin-name operation-tag*: Specifies the NQA operation to be associated with the track entry. The *admin-name* argument specifies the name of the NQA operation administrator who creates the NQA operation, and is a case-insensitive string of 1 to 32 characters. The *operation-tag* argument specifies the NQA operation tag, and is a case-insensitive string of 1 to 32 characters.

reaction *item-number*: Specifies the reaction entry to be associated with the track entry. The *item-number* argument is the reaction entry ID in the range of 1 to 10.

Usage guidelines

To create a track entry, you must specify the tracked object type, which is **nqa** in this command.

To enter the view of an existing track entry, use the **track** *track-entry-number* command. The tracked object type is not required.

To modify the settings for a track entry, execute the **undo track** command to remove the track entry, and then execute the **track nqa** command again.

Examples

Create track entry 1 and associate it with reaction entry 3 of the NQA operation **admin-test**.

```
<Sysname> system-view
[Sysname] track 1 nqa entry admin test reaction 3
[Sysname-track-1]
```

Related commands

delay

display track

Contents

Loopback MAC swap commands

Loopback MAC swap is supported only in R6348P01 and later.

display loopback swap-mac information

Use **display loopback swap-mac information** to display loopback MAC swap test information.

Syntax

display loopback swap-mac information

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display local loopback MAC swap test information.

```
<Sysname> display loopback swap-mac information
  Loopback type             : local
  Loopback state            : running
  Loopback test times(s)    : 60
  Loopback interface        : GigabitEthernet1/0/1
  Loopback output interface : GigabitEthernet1/0/2
  Loopback source MAC       : 0001-0001-0001
  Loopback destination MAC  : 0002-0002-0002
  Loopback vlan             : 10
  Loopback inner vlan       : 0
  Loopback packets          : 0
  Drop packets              : 0
```

Table 1 Command output

Field	Description
Loopback type	Loopback MAC swap test type: • **local**—Local loopback MAC swap. • **remote**—Remote loopback MAC swap.
Loopback state	Loopback MAC swap test status: • **running**—The loopback MAC swap test is started. • **stop**—The loopback MAC swap test is stopped.
Loopback test time(s)	Timeout timer for the test. If the value for this field is none, you need to manually stop the test with the relevant command.
Loopback interface	Interface that swaps the source and destination MAC addresses in the test packets.

Field	Description
Loopback output interface	Interface that loops back the test packets.
Loopback source MAC	Source MAC address that the test packets are required to match.
Loopback destination MAC	Destination MAC address that the test packets are required to match.
Loopback vlan	VLAN ID that the test packets are required to match.
Loopbck inner vlan	Inner VLAN ID that the test packets are required to match.
Loopback packets	Number of received packets that match the specified test parameters.
Drop packets	This field is not supported in the current software version. Number of dropped packets that do not match the specified test parameters.

Related commands

loopback local swap-mac

loopback remote swap-mac

loopback local swap-mac

Use **loopback local swap-mac** to configure local loopback MAC swap parameters.

Use **undo loopback local swap-mac** to delete local loopback MAC swap parameters.

Syntax

loopback local swap-mac source-mac *source-mac-address* **dest-mac** *dest-mac-address* **vlan** *vlan-id* [**inner-vlan** *inner-vlan-id*] *interface interface-type interface-number* [**timeout** { *time-value* | **none** }]

undo loopback local swap-mac

Default

Local loopback MAC swap parameters are not configured.

Views

Ethernet interface view

Predefined user roles

network-admin

network-operator

Parameters

source-mac *source-mac-address*: Specifies the source MAC address that the test packets are required to match. The MAC address must be a unicast MAC address.

dest-mac *dest-mac-address*: Specifies the destination MAC address that the test packets are required to match. The MAC address must be a unicast MAC address.

vlan *vlan-id*: Specifies the VLAN ID that the test packets are required to match, in the range of 1 to 4094.

inner-vlan *inner-vlan-id*: Specifies the inner VLAN ID that the test packets are required to match, in the range of 1 to 4094. If you do not specify this option, the device does not match the inner

VLAN ID of packets. **interface** *interface-type interface-number*: Specifies an interface by its type and number for looping back the test packets.

timeout { *time-value* | **none** }: Specifies the timeout timer for the test. After you start the loopback MAC swap test, the test automatically stops upon expiration of the timeout timer. The value range for the *time-value* argument is 5 to 300 seconds. If you specify the **none** keyword, the loopback MAC swap test does not automatically stop. You can only use the **loopback swap-mac stop** command to manually stop the test. By default, the timeout timer for the loopback MAC swap test is 60 seconds.

Usage guidelines

The device takes a packet as a test packet if its source MAC address, destination MAC address, VLAN ID, and inner VLAN ID match the settings configured in this command.

After configuring local loopback MAC swap parameters, you need to execute the **loopback swap-mac start** command to start the test. After starting the test, the tester sends test packets to the downlink interface on the tested device. The tested device swaps the source and destination MAC addresses in the test packets on the downlink interface, and then loops back the test packets to the tester through the specified interface. In this way, the network connectivity and quality information are obtained.

The test scope for local loopback MAC swap is the network from the tester to the downlink interface on the tested device (including the tested device).

Examples

Configure local loopback MAC swap parameters.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] loopback local swap-mac source-mac 00e0-fc00-0085
dest-mac 00e0-fc00-1004 vlan 100 interface gigabitethernet 1/0/2
```

loopback remote swap-mac

Use **loopback remote swap-mac** to configure remote loopback MAC swap parameters.

Use **undo loopback remote swap-mac** to delete remote loopback MAC swap parameters.

Syntax

loopback remote swap-mac source-mac *source-mac-address* **dest-mac** *dest-mac-address* **vlan** *vlan-id* [**inner-vlan** *inner-vlan-id*] [**timeout** { *time-value* | **none** }]

undo loopback remote swap-mac

Default

Remote loopback MAC swap parameters are not configured.

Views

Ethernet interface view

Predefined user roles

network-admin

network-operator

Parameters

source-mac *source-mac-address*: Specifies the source MAC address that the test packets are required to match. The MAC address must be a unicast MAC address.

dest-mac *dest-mac-address*: Specifies the destination MAC address that the test packets are required to match. The MAC address must be a unicast MAC address.

vlan *vlan-id*: Specifies the VLAN ID that the test packets are required to match, in the range of 1 to 4094.

inner-vlan *inner-vlan-id*: Specifies the inner VLAN ID that the test packets are required to match, in the range of 1 to 4094. If you do not specify this option, the device does not match the inner VLAN ID of packets.

timeout { *time-value* | **none** }: Specifies the timeout timer for the test. After you start the loopback MAC swap test, the test automatically stops upon expiration of the timeout timer. The value range for the *time-value* argument is 5 to 300 seconds. If you specify the **none** keyword, the loopback MAC swap test does not automatically stop. You can only use the **loopback swap-mac stop** command to manually stop the test. By default, the timeout timer for the loopback MAC swap test is 60 seconds.

Usage guidelines

The device takes a packet as a test packet if its source MAC address, destination MAC address, VLAN ID, and inner VLAN ID match the settings configured in this command.

After configuring remote loopback MAC swap parameters, you need to execute the **loopback swap-mac start** command to start the test. After starting the test, the tester sends test packets to the uplink interface on the tested device. The tested device swaps the source and destination MAC addresses in the test packets on the uplink interface, and then loops back the test packets to the tester through the uplink interface. In this way, the network connectivity and quality information are obtained.

The test scope for remote loopback MAC swap is the network from the tester to the uplink interface on the tested device (excluding the tested device).

Examples

Configure remote loopback MAC swap parameters.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] loopback local swap-mac source-mac 00e0-fc00-0085
dest-mac 00e0-fc00-1004 vlan 100
```

loopback swap-mac start

Use **loopback swap-mac start** to start the loopback MAC swap test.

Syntax

loopback swap-mac start

Views

Ethernet interface view

Predefined user roles

network-admin

network-operator

Usage guidelines

After configuring local or remote loopback MAC swap parameters, you need to execute the **loopback swap-mac start** command to start the test.

Both local and remote loopback MAC swap tests will affect normal operation of the network. As a best practice to minimize impact on the network, execute the **loopback swap-mac stop** command immediately to stop the test after it is completed.

Execute the **loopback swap-mac start** command again to start a new test if the previous test automatically stops upon expiration of the timeout timer or is manually stopped with the **loopback swap-mac stop** command.

Examples

Start the loopback MAC swap test.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] loopback swap-mac start
```

loopback swap-mac stop

Use **loopback swap-mac stop** to stop the loopback MAC swap test.

Syntax

loopback swap-mac stop

Views

Ethernet interface view

Predefined user roles

network-admin

network-operator

Usage guidelines

After configuring local or remote loopback MAC swap parameters, you need to execute the **loopback swap-mac start** command to start the test.

Both local and remote loopback MAC swap tests will affect normal operation of the network. As a best practice to minimize impact on the network, execute the **loopback swap-mac stop** command immediately to stop the test after it is completed.

Execute the **loopback swap-mac start** command again to start a new test if the previous test automatically stops upon expiration of the timeout timer or is manually stopped with the **loopback swap-mac stop** command.

Examples

Stop the loopback MAC swap test.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] loopback swap-mac stop
```

Network Management and Monitoring Command Reference

This command reference is applicable to the following switches and software versions:

H3C S5120V2-LI switch series (Release 6308P01 and later)
H3C S3100V3-SI switch series (Release 6309P01 and later)
H3C S5110V2 switch series (Release 6310 and later)
H3C S5110V2-SI switch series (Release 6310 and later)
H3C S5000V3-EI switch series (Release 6310 and later)
H3C S5000V5-EI switch series (Release 6319P01 and later)
H3C S5000E-X switch series (Release 6310 and later)
H3C S5130S-LI switch series (Release 6310 and later)
H3C MS4320V2 switch series (Release 6308P01 and later)
H3C MS4320 switch series (Release 6308P01 and later)
H3C MS4300V2 switch series (Release 6308P01 and later)
H3C MS4200 switch series (Release 6310 and later)
H3C WS5810-WiNet switch series (Release 6308P01 and later)
H3C WS5820-WiNet switch series (Release 6308P01 and later)
H3C WAS6000 switch series (Release 6308P01 and later)
H3C S5000X-EI switch series (Release 6329 and later)
H3C MS4320V3 switch series (Release 6329 and later)
H3C S5120V3-SI switch series (Release 6329 and later)
H3C S5120V3-LI switch series (Release 6329 and later)

New H3C Technologies Co., Ltd.
http://www.h3c.com

Software version: Release 63xx
Document version: 6W105-20230524

Preface

This command reference describes the network management and monitoring configuration commands. It covers the commands for viewing system information, collecting traffic statistics, assessing the network performance, synchronizing time for all devices with clocks in your network, and checking and debugging the current network connectivity with the ping, tracert, and debug commands.

This preface includes the following topics about the documentation:

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.

Convention	Description
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Documentation feedback

You can e-mail your comments about product documentation to info@h3c.com.

We appreciate your comments.

Contents

Ping, tracert, and system debugging commands

debugging

Use **debugging** to enable debugging for a module.

Use **undo debugging** to disable debugging for a module or for all modules.

Syntax

debugging *module-name* [*option*]

undo debugging { **all** | *module-name* [*option*] }

Default

Debugging is disabled for all modules.

Views

User view

Predefined user roles

network-admin

Parameters

module-name: Specifies a module by its name, such as **arp** or **device**. For a list of supported modules, use the **debugging ?** command.

option: Specifies the debugging option for a module. Available options vary by module. To display the debugging options supported by a module, use the **debugging** *module-name* **?** command.

all: Specifies all modules.

Usage guidelines

CAUTION:

Output of excessive debugging messages increases the CPU usage and downgrades the system performance. To guarantee system performance, enable debugging only for modules that are in an exceptional condition.

The system sends generated debug messages to the device information center, which then sends the messages to appropriate destinations based on the log output configuration. For more information about the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Enable debugging for the device management module.

```
<Sysname> debugging dev
```

Related commands

display debugging

display debugging

Use **display debugging** to display the enabled debugging features for a module or for all modules.

Syntax

display debugging [*module-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

module-name: Specifies a module by its name. For a list of supported modules, use the **display debugging ?** command. If you do not specify a module name, this command displays the enabled debugging features for all modules.

Examples

Display all enabled debugging features.

```
<Sysname> display debugging
DEV debugging switch is on
```

Related commands

debugging

ping

Use **ping** to test the reachability of the destination IP address and display ping statistics.

Syntax

ping [**ip**] [**-a** *source-ip* | **-c** *count* | **-f** | **-h** *ttl* | **-i** *interface-type interface-number* | **-m** *interval* | **-n** | **-p** *pad* | **-q** | **-r** | **-s** *packet-size* | **-t** *timeout* | **-tos** *tos* | **-v**] * *host*

Views

Any view

Predefined user roles

network-admin

Parameters

ip: Distinguishes between a destination host name and the **ping** command keywords if the name of the destination host is **i**, **ip**, **ipv**, **ipv6**, **l**, **ls**, or **lsp**. For example, you must use the command in the form of **ping ip ip** instead of **ping ip** if the destination host name is **ip**.

-a *source-ip*: Specifies an IP address of the device as the source IP address of ICMP echo requests. If this option is not specified, the source IP address of ICMP echo requests is the primary IP address of the outbound interface.

-c *count*: Specifies the number of ICMP echo requests that are sent to the destination. The value range is 1 to 4294967295, and the default is 5.

-f: Sets the "Don't Fragment" bit in the IP header.

-h *ttl*: Specifies the TTL value of ICMP echo requests. The value range is 1 to 255, and the default is 255.

-i *interface-type interface-number*: Specifies the source interface for ICMP echo requests. If you do not specify this option, the system uses the primary IP address of the matching route's egress interface as the source interface for ICMP echo requests.

-m *interval*: Specifies the interval (in milliseconds) to send ICMP echo requests. The value range is 1 to 65535, and the default is 200.

-n: Disables domain name resolution for the *host* argument. If the *host* argument represents the host name of the destination, and if this keyword is not specified, the device translates *host* into an address.

-p *pad*: Specifies the value of the **pad** field in an ICMP echo request, in hexadecimal format, 1 to 8 bits. The *pad* argument is in the range of 0 to ffffffff. If the specified value is less than 8 bits, 0s are added in front of the value to extend it to 8 bits. For example, if *pad* is configured as 0x2f, then the packets are padded with 0x0000002f to make the total length of the packet meet the requirements of the device. By default, the padded value starts from 0x01 up to 0xff, where another round starts again if necessary, such as 0x010203…feff01….

-q: Displays only the summary statistics. If this keyword is not specified, the system displays all the ping statistics.

-r: Records the addresses of the hops (up to 9) the ICMP echo requests passed. If this keyword is not specified, the addresses of the hops that the ICMP echo requests passed are not recorded.

-s *packet-size*: Specifies the length (in bytes) of ICMP echo requests (excluding the IP packet header and the ICMP packet header). The value range is 20 to 9600, and the default is 56.

-t *timeout*: Specifies the timeout time (in milliseconds) of an ICMP echo reply. The value range is 0 to 65535, and the default is 2000. If the source does not receive an ICMP echo reply within the timeout, it considers the ICMP echo reply timed out.

-tos *tos*: Specifies the ToS value of ICMP echo requests. The value range is 0 to 255, and the default is 0.

-v: Displays non-ICMP echo reply packets. If this keyword is not specified, the system does not display non-ICMP echo reply packets.

host: Specifies the IP address or host name of the destination. The host name is a case-insensitive string of 1 to 253 characters. It can contain letters, digits, and special characters such as hyphen (-), underscore (_), and dot (.).

Usage guidelines

To ping a device identified by its host name, configure the DNS settings on the device first. If the DNS settings are not configured, the ping operation fails.

To abort the ping operation during the execution of the command, press **Ctrl+C**.

Examples

Test whether the device with an IP address of 1.1.2.2 is reachable.

```
<Sysname> ping 1.1.2.2
Ping 1.1.2.2 (1.1.2.2): 56 data bytes, press CTRL_C to break
56 bytes from 1.1.2.2: icmp_seq=0 ttl=254 time=2.137 ms
56 bytes from 1.1.2.2: icmp_seq=1 ttl=254 time=2.051 ms
56 bytes from 1.1.2.2: icmp_seq=2 ttl=254 time=1.996 ms
56 bytes from 1.1.2.2: icmp_seq=3 ttl=254 time=1.963 ms
56 bytes from 1.1.2.2: icmp_seq=4 ttl=254 time=1.991 ms

--- Ping statistics for 1.1.2.2 ---
```

```
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.963/2.028/2.137/0.062 ms
```

Test whether the device with an IP address of 1.1.2.2 is reachable. Only results are displayed.

```
<Sysname> ping -q 1.1.2.2
Ping 1.1.2.2 (1.1.2.2): 56 data bytes, press CTRL_C to break

--- Ping statistics for 1.1.2.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.962/2.196/2.665/0.244 ms
```

Test whether the device with an IP address of 1.1.2.2 is reachable. The IP addresses of the hops that the ICMP packets passed in the path are displayed.

```
<Sysname> ping -r 1.1.2.2
Ping 1.1.2.2 (1.1.2.2): 56 data bytes, press CTRL_C to break
56 bytes from 1.1.2.2: icmp_seq=0 ttl=254 time=4.685 ms
RR:      1.1.2.1
         1.1.2.2
         1.1.1.2
         1.1.1.1
56 bytes from 1.1.2.2: icmp_seq=1 ttl=254 time=4.834 ms  (same route)
56 bytes from 1.1.2.2: icmp_seq=2 ttl=254 time=4.770 ms  (same route)
56 bytes from 1.1.2.2: icmp_seq=3 ttl=254 time=4.812 ms  (same route)
56 bytes from 1.1.2.2: icmp_seq=4 ttl=254 time=4.704 ms  (same route)

--- Ping statistics for 1.1.2.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 4.685/4.761/4.834/0.058 ms
```

The output shows the following information:

- The destination is reachable.
- The route is 1.1.1.1 <-> {1.1.1.2; 1.1.2.1} <-> 1.1.2.2.

Table 1 Command output

Field	Description
Ping 1.1.2.2 (1.1.2.2): 56 data bytes, press CTRL_C to break	Test whether the device with IP address 1.1.2.2 is reachable. There are 56 bytes in each ICMP echo request. Press **Ctrl+C** to abort the ping operation.
56 bytes from 1.1.2.2: icmp_seq=0 ttl=254 time=4.685 ms	Received ICMP echo replies from the device whose IP address is 1.1.2.2. If no echo reply is received within the timeout period, no information is displayed. • **bytes**—Number of bytes in the ICMP echo reply. • **icmp_seq**—Packet sequence, used to determine whether a segment is lost, disordered or repeated. • **ttl**—TTL value in the ICMP echo reply. • **time**—Response time.
RR:	Routers through which the ICMP echo request passed. They are displayed in inversed order, which means the router with a smaller distance to the destination is displayed first.
--- Ping statistics for 1.1.2.2 ---	Statistics on data received and sent in the ping operation.
5 packet(s) transmitted	Number of ICMP echo requests sent.

Field	Description
5 packet(s) received	Number of ICMP echo replies received.
0.0% packet loss	Percentage of unacknowledged packets to the total packets sent.
round-trip min/avg/max/std-dev = 4.685/4.761/4.834/0.058 ms	Minimum/average/maximum/standard deviation response time, in milliseconds.

ping ipv6

Use **ping ipv6** to test the reachability of the destination IPv6 address and display IPv6 ping statistics.

Syntax

ping ipv6 [**-a** *source-ipv6* | **-c** *count* | **-i** *interface-type interface-number* | **-m** *interval* | **-q** | **-s** *packet-size* | **-t** *timeout* | **-tc** *traffic-class*| **-v**] * *host*

Views

Any view

Predefined user roles

network-admin

Parameters

-a *source-ipv6*: Specifies an IPv6 address of the device as the source IP address of ICMP echo requests. If this option is not specified, the source IPv6 address of ICMP echo requests is the IPv6 address of the outbound interface. See RFC 3484 for information about the address selection rule.

-c *count*: Specifies the number of ICMPv6 echo requests that are sent to the destination. The value range is 1 to 4294967295, and the default is 5.

-i *interface-type interface-number*: Specifies the source interface for ICMPv6 echo requests. This option must be specified when the destination address is a multicast address or a link local address. If you do not specify this option, the system uses the primary IP address of the matching route's egress interface as the source interface for ICMPv6 echo requests.

-m *interval*: Specifies the interval (in milliseconds) to send an ICMPv6 echo reply. The value range is 1 to 65535, and the default is 1000.

-q: Displays only the summary statistics. If you do not specify this keyword, the system displays all the ping statistics.

-s *packet-size*: Specifies the length (in bytes) of ICMPv6 echo requests (excluding the IPv6 packet header and the ICMPv6 packet header). The value range is 20 to 9600, and the default is 56.

-t *timeout*: Specifies the timeout time (in milliseconds) of an ICMPv6 echo reply. The value range is 0 to 65535, and the default is 2000.

-tc *traffic-class*: Specifies the traffic class value in an ICMPv6 packet. The value range is 0 to 255 and the default is 0.

-v: Displays detailed information (including the **dst** field and the **idx** field) about ICMPv6 echo replies. If this keyword is not specified, the system only displays brief information (not including the **dst** field and the **idx** field) about ICMPv6 echo replies.

host: Specifies the IPv6 address or host name of the destination. The host name is a case-insensitive string of 1 to 253 characters. It can contain letters, digits, and special characters such as hyphen (-), underscore (_), and dot (.).

Usage guidelines

To ping a device identified by its host name, configure the DNS settings on the device first. If the DNS settings are not configured, the IPv6 ping operation fails.

To abort the IPv6 ping operation during the execution of the command, press **Ctrl+C**.

Examples

Test whether the IPv6 address (2001::2) is reachable.

```
<Sysname> ping ipv6 2001::2
Ping6(56 data bytes) 2001::1 --> 2001::2, press CTRL_C to break
56 bytes from 2001::2, icmp_seq=0 hlim=64 time=62.000 ms
56 bytes from 2001::2, icmp_seq=1 hlim=64 time=23.000 ms
56 bytes from 2001::2, icmp_seq=2 hlim=64 time=20.000 ms
56 bytes from 2001::2, icmp_seq=3 hlim=64 time=4.000 ms
56 bytes from 2001::2, icmp_seq=4 hlim=64 time=16.000 ms

--- Ping6 statistics for 2001::2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 4.000/25.000/62.000/20.000 ms
```

Test whether the IPv6 address (2001::2) is reachable. Only the statistics are displayed.

```
<Sysname> ping ipv6 –q 2001::2
Ping6(56 data bytes) 2001::1 --> 2001::2, press CTRL_C to break

--- Ping6 statistics for 2001::2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 4.000/25.000/62.000/20.000 ms
```

Test whether the IPv6 address (2001::2) is reachable. Detailed ping information is displayed.

```
<Sysname> ping ipv6 –v 2001::2
Ping6(56 data bytes) 2001::1 --> 2001::2, press CTRL_C to break
56 bytes from 2001::2, icmp_seq=0 hlim=64 dst=2001::1 idx=3 time=62.000 ms
56 bytes from 2001::2, icmp_seq=1 hlim=64 dst=2001::1 idx=3 time=23.000 ms
56 bytes from 2001::2, icmp_seq=2 hlim=64 dst=2001::1 idx=3 time=20.000 ms
56 bytes from 2001::2, icmp_seq=3 hlim=64 dst=2001::1 idx=3 time=4.000 ms
56 bytes from 2001::2, icmp_seq=4 hlim=64 dst=2001::1 idx=3 time=16.000 ms

--- Ping6 statistics for 2001::2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 4.000/25.000/62.000/20.000 ms
```

Table 2 Command output

Field	Description
Ping6(56 data bytes) 2001::1 --> 2001::2, press CTRL_C to break	An ICMPv6 echo reply with a data length of 56 bytes is sent from 2001::1 to 2001::2. Press **Ctrl+C** to abort the IPv6 ping operation.

Field	Description
56 bytes from 2001::2, icmp_seq=1 hlim=64 dst=2001::1 idx=3 time=62.000 ms	Received ICMPv6 echo replies from the device whose IPv6 address is 2001::2. • The number of data bytes is 56. • The packet sequence is 1. • The hop limit value is 64. • The destination address is 2001::1. Specify the **-v** keyword to display this field. • The index for the packet inbound interface is 3. Specify the **-v** keyword to display this field. • The response time is 62 milliseconds.
--- Ping6 statistics for 2001::2 ------	Statistics on data received and sent in an IPv6 ping operation.
5 packet(s) transmitted	Number of ICMPv6 echo requests sent.
5 packet(s) received	Number of ICMPv6 echo replies received.
0.0% packet loss	Percentage of unacknowledged packets to the total packets sent.
round-trip min/avg/max/ std-dev =4.000/25.000/62.000/20.000 ms	Minimum/average/maximum/standard deviation response time, in milliseconds.

tracert

Use **tracert** to trace the path that the packets traverse from source to destination.

Syntax

tracert [**-a** *source-ip* | **-f** *first-ttl* | **-m** *max-ttl* | **-p** *port* | **-q** *packet-number* | **-t** *tos* | **-w** *timeout*] * *host*

Views

Any view

Predefined user roles

network-admin

Parameters

-a *source-ip*: Specifies an IP address of the device as the source IP address of probe packets. If this option is not specified, the source IP address of probe packets is the primary IP address of the outbound interface.

-f *first-ttl*: Specifies the TTL of the first packet sent to the destination. The value range is 1 to 255, and the default is 1. It must be no greater than the value of the *max-ttl* argument.

-m *max-ttl*: Specifies the maximum number of hops allowed for a probe packet. The value range is 1 to 255, and the default is 30. It must be no smaller than the value of the *first-ttl* argument.

-p *port*: Specifies an invalid UDP port of the destination. The value range is 1 to 65535, and the default is 33434.

-q *packet-number*: Specifies the number of probe packets to send per hop. The value range is 1 to 65535, and the default is 3.

-t *tos*: Specifies the ToS value of probe packets. The value range is 0 to 255, and the default is 0.

-w *timeout*: Specifies the timeout time in milliseconds of the reply packet for a probe packet. The value range is 1 to 65535, and the default is 5000.

host: Specifies the IP address or host name of the destination. The host name is a case-insensitive string of 1 to 253 characters. It can contain letters, digits, and special characters such as hyphen (-), underscore (_), and dot (.).

Usage guidelines

After identifying network failure with the **ping** command, use the **tracert** command to locate failed nodes.

The output from the **tracert** command includes IP addresses of all the Layer 3 devices that the packets traverse from source to destination. Asterisks (* * *) are displayed if the device cannot reply with an ICMP error message. The reason might be the destination is unreachable or sending ICMP timeout/destination unreachable packets is disabled.

Before starting a tracert operation, you must enable sending of ICMP destination unreachable messages on the intermediate devices between the source and destination. The tracert operation stops if any one of the following ICMP destination unreachable messages is received:

- **!N**—Network unreachable.
- **!H**—Destination host unreachable.
- !**P**—Protocol unreachable. The protocol number is unknown.
- **!F**—Fragmentation needed. This message indicates that packet fragmentation is needed but the "Don't Fragment" bit is set on an immediate device.
- **!W**—Destination host unknown.
- **!Q**—Network unreachable for ToS.
- **!T**—Host unreachable for ToS.
- **!X**—Communication administratively prohibited by filtering policies.
- **!V**—Host precedence violation.
- **!C**—Precedence cutoff in effect.

To abort the tracert operation during the execution of the command, press **Ctrl+C**.

Examples

Display the path that the packets traverse from source to destination (1.1.2.2).

```
<Sysname> tracert 1.1.2.2
traceroute to 1.1.2.2 (1.1.2.2), 30 hops at most, 40 bytes each packet, press CTRL_C to break
 1  1.1.1.2 (1.1.1.2) 673 ms 425 ms 30 ms
 2  1.1.2.2 (1.1.2.2) [AS 100] 580 ms 470 ms 80 ms
```

Table 3 Command output

Field	Description
traceroute to 1.1.2.2 (1.1.2.2)	Display the route that the IP packets traverse from the current device to the device whose IP address is 1.1.2.2.
hops at most	Maximum number of hops of the probe packets, which can be set by the **-m** keyword.
bytes each packet	Number of bytes of a probe packet.
press CTRL_C to break	During the execution of the command, press **Ctrl+C** to abort the tracert operation.

Field	Description
2 1.1.2.2 (1.1.2.2) [AS 100] 580 ms 470 ms 80 ms	Probe result of the probe packets that contain a TTL value of 2, including the following information about the second hop: • Domain name of the hop. If no domain name is configured, the IP address is displayed as the domain name. • IP address of the hop. The IP address is displayed in parentheses. • Number of the AS that the hop belongs to. The AS number appears only when it is found for the hop in the specified routing table. • The round-trip time of the probe packets. The number of packets that can be sent in each probe can be set by using the **-q** keyword.

tracert ipv6

Use **tracert ipv6** to display the path that the IPv6 packets traverse from source to destination.

Syntax

tracert ipv6 [**-f** *first-hop* | **-m** *max-hops* | **-p** *port* | **-q** *packet-number* | **-t** *traffic-class* | **-w** *timeout*] * *host*

Views

Any view

Predefined user roles

network-admin

Parameters

-f *first-hop*: Specifies the TTL value of the first packet. The value range is 1 to 255, and the default is 1. The value must be no greater than the value of the *max-hops* argument.

-m *max-hops*: Specifies the maximum number of hops allowed for a packet. The value range is 1 to 255, and the default is 30. The value must be no smaller than the value of the *first-hop* argument.

-p *port*: Specifies an invalid UDP port of the destination. The value range is 1 to 65535, and the default is 33434.

-q *packet-number*: Specifies the number of probe packets sent each time. The value range is 1 to 65535, and the default is 3.

-t *traffic-class*: Specifies the traffic class value in an IPv6 probe packet. The value range is 0 to 255, and the default is 0.

-w *timeout*: Specifies the timeout time (in milliseconds) of the reply packet of a probe packet. The value range is 1 to 65535, and the default is 5000.

host: Specifies the IPv6 address or host name of the destination. The host name is a case-insensitive string of 1 to 253 characters. It can contain letters, digits, and special characters such as hyphen (-), underscore (_), and dot (.).

Usage guidelines

After identifying network failure with the **ping ipv6** command, you can use the **tracert ipv6** command to locate failed nodes.

The output from the **tracert ipv6** command includes IPv6 addresses of all the Layer 3 devices that the packets traverse from source to destination. Asterisks (* * *) are displayed if the device

cannot reply with an ICMP error message. The reason might be the destination is unreachable or sending ICMP timeout/destination unreachable packets is disabled.

Before starting an IPv6 tracert operation, you must enable sending of ICMPv6 destination unreachable messages on the intermediate devices between the source and destination. The IPv6 tracert operation stops if any one of the following ICMPv6 destination unreachable messages is received:

- **!N**—No route to destination.
- **!P**—Communication with destination administratively prohibited by filtering policies.
- **!A**—Address unreachable. The unreachable reason is unknown.
- **!S**—Beyond scope of source address. This message is displayed if the probe packet has a link-local source address and a non-link-local destination address. Such a packet cannot be delivered to the destination without leaving the scope of the source address.

To abort the tracert operation during the execution of the command, press **Ctrl+C**.

Examples

Display the path that the packets traverse from source to destination (2001:3::2).

```
<Sysname> tracert ipv6 2001:3::2
traceroute to 2001:3::2(2001:3::2), 30 hops at most, 60 byte packets, press CTRL_C to break
 1  2001:1::2  0.661 ms  0.618 ms  0.579 ms
 2  2001:2::2 [AS 100]  0.861 ms  0.718 ms  0.679 ms
 3  2001:3::2 [AS 200]  0.822 ms  0.731 ms  0.708 ms
```

Table 4 Command output

Field	Description
traceroute to 2001:3::2	Display the route that the IPv6 packets traverse from the current device to the device whose IP address is 2001:3:2.
hops at most	Maximum number of hops of the probe packets, which can be set by the **-m** keyword.
byte packets	Number of bytes of a probe packet.
2 2001:2::2 [AS 100] 0.861 ms 0.718 ms 0.679 ms	Probe result of the probe packets that contain a hoplimit value of 2, including the following information about the second hop: • IPv6 address of the hop. • Number of the AS the hop belongs to. The AS number appears only when it is found for the hop in the specified routing table. • The round-trip time of the probe packets. The number of packets that can be sent in each probe can be set by using the **-q** keyword.

Contents

NQA commands

NQA client commands

advantage-factor

Use **advantage-factor** to set the advantage factor to be used for calculating Mean Opinion Scores (MOS) and Calculated Planning Impairment Factor (ICPIF) values.

Use **undo advantage-factor** to restore the default.

Syntax

advantage-factor *factor*

undo advantage-factor

Default

The advantage factor is 0.

Views

Voice operation view

Predefined user roles

network-admin

Parameters

factor: Specifies the advantage factor in the range of 0 to 20.

Usage guidelines

The evaluation of voice quality depends on users' tolerance for voice quality. For users with higher tolerance for voice quality, use the **advantage-factor** command to set an advantage factor. When the system calculates the ICPIF value, it subtracts the advantage factor to modify ICPIF and MOS values for voice quality evaluation.

Examples

Set the advantage factor to 10 for the voice operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type voice
[Sysname-nqa-admin-test-voice] advantage-factor 10
```

codec-type

Use **codec-type** to configure the codec type for the voice operation.

Use **undo codec-type** to restore the default.

Syntax

codec-type { **g711a** | **g711u** | **g729a** }

undo codec-type

Default

The codec type for the voice operation is G.711 A-law.

Views

Voice operation view

Predefined user roles

network-admin

Parameters

g711a: Specifies G.711 A-law codec type.

g711u: Specifies G.711 μ-law codec type

g729a: Specifies G.729 A-law codec type.

Examples

Set the codec type to **g729a** for the voice operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type voice
[Sysname-nqa-admin-test-voice] codec-type g729a
```

community read

Use **community read** to specify the community name for the SNMP operation.

Use **undo community read** to restore the default.

Syntax

community read { **cipher** | **simple** } *community-name*

undo community read

Default

The SNMP operation uses the community name **public**.

Views

SNMP operation view

Predefined user roles

network-admin

Parameters

cipher: Specifies a community name in encrypted form.

simple: Specifies a community name in plaintext form. For security purposes, the community name specified in plaintext form will be stored in encrypted form.

community-name: Specifies the community name. Its plaintext form is a case-sensitive string of 1 to 32 characters. Its encrypted form is a case-sensitive string of 33 to 73 characters.

Usage guidelines

You must specify the community name for the SNMP operation when both of the following conditions exist:

- The SNMP operation uses the SNMPv1 or SNMPv2c agent.
- The SNMPv1 or SNMPv2c agent is configured with a read-only or read-write community name.

The specified community name must be the same as the community name configured on the SNMP agent.

The community name configuration is not required if the SNMP operation uses the SNMPv3 agent.

For more information about SNMP, see "Configuring SNMP."

Examples

Specify **readaccess** as the community name for the SNMP operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type snmp
[Sysname-nqa-admin-test-snmp] community read simple readaccess
```

data-fill

Use **data-fill** to configure the payload fill string for probe packets.

Use **undo data-fill** to restore the default.

Syntax

data-fill *string*

undo data-fill

Default

The default payload fill string is the hexadecimal string 00010203040506070809.

Views

ICMP/UDP echo operation view

Path jitter/UDP jitter/voice operation view

ICMP/TCP/UDP template view

Predefined user roles

network-admin

Parameters

string: Specifies a case-sensitive string of 1 to 200 characters.

Usage guidelines

If the payload length is smaller than the string length, only the first part of the string is filled. For example, if you configure the string as **abcd** and set the payload size to 3 bytes, **abc** is filled.

If the payload length is greater than the string length, the system fills the payload with the string cyclically until the payload is full. For example, if you configure the string as **abcd** and the payload size as 6 bytes, **abcdab** is filled.

How the string is filled depends on the operation type.

- For the ICMP echo operation, the string fills the whole payload of an ICMP echo request.
- For the UDP echo operation, the first five bytes of the payload of a UDP packet are for special purpose. The string fills the remaining part of payload.
- For the UDP jitter operation, the first 68 bytes of the payload of a UDP packet are for special purpose. The string fills the remaining part of the payload.
- For the voice operation, the first 16 bytes of the payload of a UDP packet are for special purpose. The string fills the remaining part of the payload.

- For the path jitter operation, the first four bytes of the payload of an ICMP echo request are for special purpose. The string fills the remaining part of payload.

Examples

Specify **abcd** as the payload fill string for ICMP echo requests.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] data-fill abcd
```

In TCP template view, specify **abcd** as the payload fill string for probe packets.

```
<Sysname> system-view
[Sysname] nqa template tcp tcptplt
[Sysname-nqatplt-tcp-tcptplt] data-fill abcd
```

data-size

Use **data-size** to set the payload size for each probe packet.

Use **undo data-size** to restore the default.

Syntax

data-size *size*

undo data-size

Default

The default payload size of a probe packet for different operations is described in Table 1.

Table 1 Default payload size of a probe packet

Operation type	Codec type	Default size (bytes)
ICMP echo	N/A	100
UDP echo	N/A	100
UDP jitter	N/A	100
UDP tracert	N/A	100
Path jitter	N/A	100
Voice	G.711 A-law	172
Voice	G.711 μ-law	172
Voice	G.729 A-law	32

Views

ICMP/UDP echo operation view

UDP tracert operation view

Path jitter/UDP jitter/voice operation view

ICMP/UDP template view

Predefined user roles

network-admin

Parameters

size: Specifies the payload size. Available value ranges include:

- 20 to 65507 bytes for the ICMP echo, UDP echo, or UDP tracert operation.
- 68 to 65507 bytes for the UDP jitter or path jitter operation.
- 16 to 65507 bytes for the voice operation.

Usage guidelines

In ICMP echo and path jitter operations, the command sets the payload size for each ICMP echo request.

In UDP echo, UDP jitter, UDP tracert, and voice operations, the command sets the payload size for each UDP packet.

Examples

Set the payload size to 80 bytes for each ICMP echo request.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] data-size 80
```

In ICMP template view, set the payload size to 80 bytes for each probe packet.

```
<Sysname> system-view
[Sysname] nqa template icmp icmptplt
[Sysname-nqatplt-icmp-icmptplt] data-size 80
```

description

Use **description** to configure a description for an NQA operation, such as the operation type or purpose.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

No description is configured for an NQA operation.

Views

Any NQA operation view

Any NQA template view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 200 characters.

Examples

Configure the description as **icmp-probe** for the ICMP echo operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
```

```
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] description icmp-probe
```

In ICMP template view, configure the description as **icmp-probe** for the NQA operation.

```
<Sysname> system-view
[Sysname] nqa template icmp icmptplt
[Sysname-nqatplt-icmp-icmptplt] description icmp-probe
```

destination host

Use **destination host** to configure the destination host name for the operation.

Use **undo destination host** to restore the default.

Syntax

destination host *host-name*

undo destination host

Default

No destination host name is configured for the operation.

Views

UDP tracert operation view

Predefined user roles

network-admin

Parameters

host-name: Specifies the destination host name, a case-sensitive string of 1 to 254 characters. The host name can contain letters, digits, hyphens (-), underscores (_), and dots (.), but consecutive dots (.) are not allowed. If the host name is a series of dot-separated labels, each label can contain a maximum of 63 characters.

Examples

Specify **www.test.com** as the destination host name for the UDP tracert operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-tracert
[Sysname-nqa-admin-test-udp-tracert] destination host www.test.com
```

destination ip

Use **destination ip** to configure the destination IPv4 address for the operation.

Use **undo destination ip** to restore the default.

Syntax

destination ip *ip-address*

undo destination ip

Default

No destination IPv4 address is configured for an operation.

Views

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/SNMP operation view

UDP tracert operation view

ICMP jitter/path jitter/UDP jitter/voice operation view

DNS/ICMP/RADIUS/SSL/TCP/TCP half open/UDP template view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the destination IPv4 address for the operation.

Examples

Specify 10.1.1.1 as the destination IPv4 address for the ICMP echo operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] destination ip 10.1.1.1
```

In ICMP template view, specify 10.1.1.1 as the destination IPv4 address for the ICMP echo operation.

```
<Sysname> system-view
[Sysname] nqa template icmp icmptplt
[Sysname-nqatplt-icmp-icmptplt] destination ip 10.1.1.1
```

destination ipv6

Use **destination ipv6** to configure the destination IPv6 address for the operation.

Use **undo destination ipv6** to restore the default.

Syntax

destination ipv6 *ipv6-address*

undo destination ipv6

Default

No destination IPv6 address is configured for an operation.

Views

ICMP echo operation view

DNS/ICMP/RADIUS/SSL/TCP/TCP half open/UDP template view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the destination IPv6 address for the operation. IPv6 link-local addresses are not supported.

Examples

Specify 1::1 as the destination IPv6 address for the ICMP echo operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] destination ipv6 1::1
```

In ICMP template view, specify 1::1 as the destination IPv6 address for the operation.

```
<Sysname> system-view
[Sysname] nqa template icmp icmptplt
[Sysname-nqatplt-icmp-icmptplt] destination ipv6 1::1
```

destination port

Use **destination port** to configure the destination port number for the operation.

Use **undo destination port** to restore the default.

Syntax

destination port *port-number*

undo destination port

Default

The destination port number is 33434 for the UDP tracert operation and 161 for the SNMP operation.

No destination port number is configured for other types of operations.

The destination port numbers for the operations that use the following NQA templates are:

- 53 for the DNS template.
- 1812 for the RADIUS template.

No destination port number is configured for other types of NQA templates.

Views

TCP/UDP echo operation view

UDP tracert operation view

UDP jitter/voice operation view

DNS/RADIUS/SSL/TCP/UDP template view

Predefined user roles

network-admin

Parameters

port-number: Specifies the destination port number for the operation, in the range of 1 to 65535.

Examples

Set the destination port number to 9000 for the UDP echo operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-echo
[Sysname-nqa-admin-test-udp-echo] destination port 9000
```

In TCP template view, set the destination port number to 9000 for the NQA operation.

```
<Sysname> system-view
[Sysname] nqa template tcp tcptplt
[Sysname-nqatplt-tcp-tcptplt] destination port 9000
```

display nqa history

Use **display nqa history** to display the history records of NQA operations.

Syntax

display nqa history [*admin-name operation-tag*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

admin-name operation-tag: Specifies an NQA operation by its administrator name and operation tag. The *admin-name* argument represents the name of the administrator who creates the NQA operation. The *operation-tag* argument represents the operation tag. Each of the arguments is a case-insensitive string of 1 to 32 characters that cannot contain hyphens (-). If you do not specify an NQA operation, the command displays the history records of all NQA operations.

Usage guidelines

The **display nqa history** command does not display the results or statistics of the following operations:

- ICMP jitter.
- Path jitter.
- UDP jitter.
- Voice.

To view the results or statistics of the ICMP jitter, path jitter, UDP jitter, and voice operations, use the **display nqa result** or **display nqa statistics** command.

Examples

Display the history records of the UDP tracert operation with administrator name **administrator** and operation tag **tracert**.

```
<Sysname> display nqa history administrator tracert
NQA entry (admin administrator, tag tracert) history records:
Index      TTL  Response  Hop IP          Status          Time
1          2    328       4.1.1.1         Succeeded       2013-09-09 14:46:06.2
1          2    328       4.1.1.1         Succeeded       2013-09-09 14:46:05.2
1          2    328       4.1.1.1         Succeeded       2013-09-09 14:46:04.2
1          1    328       3.1.1.2         Succeeded       2013-09-09 14:46:03.2
1          1    328       3.1.1.1         Succeeded       2013-09-09 14:46:02.2
1          1    328       3.1.1.1         Succeeded       2013-09-09 14:46:01.2
```

Display the history records of the NQA operation with administrator name **administrator** and operation tag **test**.

```
<Sysname> display nqa history administrator test
NQA entry (admin administrator, tag test) history records:
  Index      Response     Status           Time
  10         329          Succeeded        2011-04-29 20:54:26.5
  9          344          Succeeded        2011-04-29 20:54:26.2
  8          328          Succeeded        2011-04-29 20:54:25.8
```

```
7           328           Succeeded        2011-04-29 20:54:25.5
6           328           Succeeded        2011-04-29 20:54:25.1
5           328           Succeeded        2011-04-29 20:54:24.8
4           328           Succeeded        2011-04-29 20:54:24.5
3           328           Succeeded        2011-04-29 20:54:24.1
2           328           Succeeded        2011-04-29 20:54:23.8
1           328           Succeeded        2011-04-29 20:54:23.4
```

Table 2 Command output

Field	Description
Index	History record ID. The history records in one UDP tracert operation have the same ID.
TTL	If the routing table bypass feature is not enabled in the operation, this field displays the TTL value in the probe packet. If the routing table bypass feature is enabled, this field value varies by the **init-ttl** command. However, the actual TTL value in the probe packet is fixed at 1.
Response	Round-trip time if the operation succeeds, timeout time upon timeout, or 0 if the operation cannot be completed, in milliseconds.
Hop IP	IP address of the node that sent the reply packet.
Status	Status of the operation result: • Succeeded. • Unknown error. • Internal error. • Timeout.
Time	Time when the operation was completed.

display nqa reaction counters

Use **display nqa reaction counters** to display the current monitoring results of reaction entries.

Syntax

display nqa reaction counters [*admin-name operation-tag* [*item-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

admin-name operation-tag: Specifies an NQA operation by its administrator name and operation tag. The *admin-name* argument represents the name of the administrator who creates the NQA operation. The *operation-tag* argument represents the operation tag. Each of the arguments is a case-insensitive string of 1 to 32 characters that cannot contain hyphens (-). If you do not specify an NQA operation, the command displays the current monitoring results of reaction entries for all NQA operations.

item-number: Specifies a reaction entry by its ID in the range of 1 to 10. If you do not specify a reaction entry, the command displays the results of all reaction entries.

Usage guidelines

The result fields display hyphens (-) in one of the following conditions:

- The threshold type is the average value.
- The monitored performance metric is ICPIF or MOS of the voice operation.

The monitoring results of an operation are accumulated, and are not cleared after the operation completes.

Examples

Display the monitoring results of all reaction entries of the ICMP echo operation with administrator name **admin** and operation tag **test**.

```
<Sysname> display nqa reaction counters admin test
NQA entry (admin admin, tag test) reaction counters:
  Index  Checked Element  Threshold Type  Checked Num  Over-threshold Num
  1      probe-duration   accumulate      12           4
  2      probe-duration   average         -            -
  3      probe-duration   consecutive     160          56
  4      probe-fail       accumulate      12           0
  5      probe-fail       consecutive     162          2
```

Table 3 Command output

Field	Description
Index	ID of a reaction entry.
Checked Element	Monitored performance metric. The available performance metrics vary by NQA operation type. For more information, see Table 4 and Table 5.
Threshold Type	Threshold type.
Checked Num	Number of targets that have been monitored for data collection.
Over-threshold Num	Number of threshold violations.

Table 4 Monitored performance metrics for DHCP/DLSw/DNS/FTP/HTTP/ICMP echo/SNMP/TCP/UDP echo operations

Monitored performance metric	Threshold type	Collect data in	Checked Num	Over-threshold Num
probe-duration	accumulate	Probes after the operation starts.	Number of completed probes.	Number of probes with duration exceeding the threshold.
	average	N/A	N/A	N/A
	consecutive	Probes after the operation starts.	Number of completed probes.	Number of probes with duration exceeding the threshold.
probe-fail	accumulate	Probes after the operation starts.	Number of completed probes.	Number of probe failures.

Monitored performance metric	Threshold type	Collect data in	Checked Num	Over-threshold Num
	consecutive	Probes after the operation starts.	Number of completed probes.	Number of probe failures.

Table 5 Monitored performance metrics for ICMP jitter/UDP jitter/voice operations

Monitored performance metric	Threshold type	Collect data in	Checked Num	Over-threshold Num
RTT	accumulate	Packets sent after the operation starts.	Number of sent packets.	Number of packets with round-trip time exceeding threshold.
	average	N/A	N/A	N/A
jitter-DS/jitter-SD	accumulate	Packets sent after the operation starts.	Number of sent packets.	Number of packets with the one-way jitter exceeding the threshold.
	average	N/A	N/A	N/A
OWD-DS/OWD-SD	N/A	Packets sent after the operation starts.	Number of sent packets.	Number of packets with the one-way delay exceeding the threshold.
packet-loss	accumulate	Packets sent after the operation starts.	Number of sent packets.	Total packet loss.
ICPIF/MOS (available only for the voice operation)	N/A	N/A	N/A	N/A

display nqa result

Use **`display nqa result`** to display the most recent result of an NQA operation.

Syntax

`display nqa result` [*`admin-name operation-tag`*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

`admin-name operation-tag`: Specifies an NQA operation by its administrator name and operation tag. The *`admin-name`* argument represents the name of the administrator who creates the NQA operation. The *`operation-tag`* argument represents the operation tag. Each of the arguments is a case-insensitive string of 1 to 32 characters that cannot contain hyphens (-). If you do not specify an NQA operation, the command displays the most recent results of all NQA operations.

Examples

Display the most recent result of the TCP operation with administrator name **admin** and operation tag **test**.

```
<Sysname> display nqa result admin test
NQA entry (admin admin, tag test) test results:
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 35/35/35
    Square-Sum of round trip time: 1225
    Last succeeded probe time: 2011-05-29 10:50:33.2
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to disconnect: 0
    Failures due to no connection: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

Display the most recent result of the ICMP jitter operation with administrator name **admin** and operation tag **test**.

```
<Sysname> display nqa result admin test
NQA entry (admin admin, tag test) test results:
    Send operation times: 10             Receive response times: 10
    Min/Max/Average round trip time: 1/2/1
    Square-Sum of round trip time: 13
    Last packet received time: 2015-03-09 17:40:29.8
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
  ICMP-jitter results:
   RTT number: 10
    Min positive SD: 0                   Min positive DS: 0
    Max positive SD: 0                   Max positive DS: 0
    Positive SD number: 0                Positive DS number: 0
    Positive SD sum: 0                   Positive DS sum: 0
    Positive SD average: 0               Positive DS average: 0
    Positive SD square-sum: 0            Positive DS square-sum: 0
    Min negative SD: 1                   Min negative DS: 2
    Max negative SD: 1                   Max negative DS: 2
    Negative SD number: 1                Negative DS number: 1
    Negative SD sum: 1                   Negative DS sum: 2
    Negative SD average: 1               Negative DS average: 2
    Negative SD square-sum: 1            Negative DS square-sum: 4
    SD average: 1                        DS average: 2
  One way results:
    Max SD delay: 1                      Max DS delay: 2
```

```
    Min SD delay: 1                         Min DS delay: 2
    Number of SD delay: 1                   Number of DS delay: 1
    Sum of SD delay: 1                      Sum of DS delay: 2
    Square-Sum of SD delay: 1               Square-Sum of DS delay: 4
    Lost packets for unknown reason: 0
```

Display the most recent result of the UDP jitter operation with administrator name **admin** and operation tag **test**.

```
<Sysname> display nqa result admin test
NQA entry (admin admin, tag test) test results:
    Send operation times: 10             Receive response times: 10
    Min/Max/Average round trip time: 15/46/26
    Square-Sum of round trip time: 8103
    Last packet received time: 2011-05-29 10:56:38.7
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
  UDP-jitter results:
   RTT number: 10
    Min positive SD: 8                      Min positive DS: 8
    Max positive SD: 18                     Max positive DS: 8
    Positive SD number: 5                   Positive DS number: 2
    Positive SD sum: 75                     Positive DS sum: 32
    Positive SD average: 15                 Positive DS average: 16
    Positive SD square-sum: 1189            Positive DS square-sum: 640
    Min negative SD: 8                      Min negative DS: 1
    Max negative SD: 24                     Max negative DS: 30
    Negative SD number: 4                   Negative DS number: 7
    Negative SD sum: 56                     Negative DS sum: 99
    Negative SD average: 14                 Negative DS average: 14
    Negative SD square-sum: 946             Negative DS square-sum: 1495
    SD average: 14                          DS average: 14
  One way results:
    Max SD delay: 22                        Max DS delay: 23
    Min SD delay: 7                         Min DS delay: 7
    Number of SD delay: 10                  Number of DS delay: 10
    Sum of SD delay: 125                    Sum of DS delay: 132
    Square-Sum of SD delay: 1805            Square-Sum of DS delay: 1988
    SD lost packets: 0                      DS lost packets: 0
    Lost packets for unknown reason: 0
```

Display the most recent result of the voice operation with administrator name **admin** and operation tag **test**.

```
<Sysname> display nqa result admin test
NQA entry (admin admin, tag test) test results:
    Send operation times: 1000           Receive response times: 0
```

```
    Min/Max/Average round trip time: 0/0/0
    Square-Sum of round trip time: 0
    Last packet received time: 0-00-00 00:00:00.0
  Extended results:
    Packet loss ratio: 100%
    Failures due to timeout: 1000
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
  Voice results:
   RTT number: 0
    Min positive SD: 0                    Min positive DS: 0
    Max positive SD: 0                    Max positive DS: 0
    Positive SD number: 0                 Positive DS number: 0
    Positive SD sum: 0                    Positive DS sum: 0
    Positive SD average: 0                Positive DS average: 0
    Positive SD square-sum: 0             Positive DS square-sum: 0
    Min negative SD: 0                    Min negative DS: 0
    Max negative SD: 0                    Max negative DS: 0
    Negative SD number: 0                 Negative DS number: 0
    Negative SD sum: 0                    Negative DS sum: 0
    Negative SD average: 0                Negative DS average: 0
    Negative SD square-sum: 0             Negative DS square-sum: 0
    SD average: 0                         DS average: 0
  One way results:
    Max SD delay: 0                       Max DS delay: 0
    Min SD delay: 0                       Min DS delay: 0
    Number of SD delay: 0                 Number of DS delay: 0
    Sum of SD delay: 0                    Sum of DS delay: 0
    Square-Sum of SD delay: 0             Square-Sum of DS delay: 0
    SD lost packets: 0                    DS lost packets: 0
    Lost packets for unknown reason: 1000
  Voice scores:
    MOS value: 0.99                       ICPIF value: 87
```

Display the most recent result of the path jitter operation with administrator name **admin** and operation tag **test**.

```
<Sysname> display nqa result admin test
NQA entry (admin admin, tag test) test results:
  Hop IP 192.168.40.210
    Basic Results:
      Send operation times: 10
      Receive response times: 10
      Min/Max/Average round trip time: 1/1/1
      Square-Sum of round trip time: 10
    Extended Results:
      Packet loss ratio: 0%
      Failures due to timeout: 0
```

```
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packets out of sequence: 0
      Packets arrived late: 0
    Path-Jitter Results:
      Jitter number: 9
        Min/Max/Average jitter: 0/0/0
      Positive jitter number: 0
        Min/Max/Average positive jitter: 0/0/0
        Sum/Square-Sum positive jitter: 0/0
      Negative jitter number: 0
        Min/Max/Average negative jitter: 0/0/0
        Sum/Square-Sum negative jitter: 0/0
  Hop IP 192.168.50.209
    Basic Results:
      Send operation times: 10
      Receive response times: 10
      Min/Max/Average round trip time: 1/1/1
      Square-Sum of round trip time: 10
    Extended Results:
      Packet loss ratio: 0%
      Failures due to timeout: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packets out of sequence: 0
      Packets arrived late: 0
    Path-Jitter Results:
      Jitter number: 9
        Min/Max/Average jitter: 0/0/0
      Positive jitter number: 0
        Min/Max/Average positive jitter: 0/0/0
        Sum/Square-Sum positive jitter: 0/0
      Negative jitter number: 0
        Min/Max/Average negative jitter: 0/0/0
        Sum/Square-Sum negative jitter: 0/0
```

Display the most recent result of the UDP tracert operation with administrator name **admin** and operation tag **test**.

```
<Sysname> display nqa result admin test
NQA entry (admin admin, tag test) test results:
    Send operation times: 6              Receive response times: 6
    Min/Max/Average round trip time: 35/35/35
    Square-Sum of round trip time: 1225
    Last succeeded probe time: 2013-09-09 14:23:24.5
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

```
UDP-tracert results:
  TTL     Hop IP              Time
  1       3.1.1.1             2013-09-09 14:23:24.5
  2       4.1.1.1             2013-09-09 14:23:24.5
```

Table 6 Command output

Field	Description
Data collecting in progress	The operation is in progress.
Send operation times	Number of operations.
Receive response times	Number of response packets received.
Min/Max/Average round trip time	Minimum/maximum/average round-trip time in milliseconds.
Square-Sum of round trip time	Square sum of round-trip time.
Last succeeded probe time	Time when the last successful probe was completed. If no probes are successful in an operation, the field displays **0**. This field is not available for UDP jitter, path jitter, and voice operations.
Last packet received time	Time when the last response packet was received. If no response packets in a probe were received, the field displays **0**. This field is available only for UDP jitter and voice operations.
Packet loss ratio	Average packet loss ratio.
Failures due to timeout	Number of timeout occurrences in an operation.
Failures due to disconnect	Number of disconnections by the peer.
Failures due to no connection	Number of failures to connect with the peer.
Failures due to internal error	Number of failures due to internal errors.
Failures due to other errors	Failures due to other errors.
Packets out of sequence	Number of failures due to out-of-sequence packets.
ICMP-jitter results	ICMP jitter operation results. This field is available only for the ICMP jitter operation.
Packets arrived late	Number of response packets received after a probe times out.
UDP-jitter results	UDP jitter operation results. This field is available only for the UDP jitter operation.
Voice results	Voice operation results. This field is available only for the voice operation.
RTT number	Number of response packets received.
Min positive SD	Minimum positive jitter from source to destination.
Min positive DS	Minimum positive jitter from destination to source.
Max positive SD	Maximum positive jitter from source to destination.
Max positive DS	Maximum positive jitter from destination to source.
Positive SD number	Number of positive jitters from source to destination.

Field	Description
Positive DS number	Number of positive jitters from destination to source.
Positive SD sum	Sum of positive jitters from source to destination.
Positive DS sum	Sum of positive jitters from destination to source.
Positive SD average	Average positive jitters from source to destination.
Positive DS average	Average positive jitters from destination to source.
Positive SD square-sum	Square sum of positive jitters from source to destination.
Positive DS square-sum	Square sum of positive jitters from destination to source.
Min negative SD	Minimum absolute value among negative jitters from source to destination.
Min negative DS	Minimum absolute value among negative jitters from destination to source.
Max negative SD	Maximum absolute value among negative jitters from source to destination.
Max negative DS	Maximum absolute value among negative jitters from destination to source.
Negative SD number	Number of negative jitters from source to destination.
Negative DS number	Number of negative jitters from destination to source.
Negative SD sum	Sum of absolute values of negative jitters from source to destination.
Negative DS sum	Sum of absolute values of negative jitters from destination to source.
Negative SD average	Average absolute value of negative jitters from source to destination.
Negative DS average	Average absolute value of negative jitters from destination to source.
Negative SD square-sum	Square sum of negative jitters from source to destination.
Negative DS square-sum	Square sum of negative jitters from destination to source.
SD average	Average value of jitters from source to destination.
DS average	Average value of jitters from destination to source.
One way results	Unidirectional delay. This field is available only for the ICMP jitter, UDP jitter, and voice operations.
Max SD delay	Maximum delay from source to destination.
Max DS delay	Maximum delay from destination to source.
Min SD delay	Minimum delay from source to destination.
Min DS delay	Minimum delay from destination to source.
Number of SD delay	Number of delays from source to destination.
Number of DS delay	Number of delays from destination to source.

Field	Description
Sum of SD delay	Sum of delays from source to destination.
Sum of DS delay	Sum of delays from destination to source.
Square-Sum of SD delay	Square sum of delays from source to destination.
Square-Sum of DS delay	Square sum of delays from destination to source.
SD lost packets	Number of lost packets from the source to the destination.
DS lost packets	Number of lost packets from the destination to the source.
Lost packets for unknown reason	Number of lost packets for unknown reasons.
Voice scores	Voice parameters. This field is available only for the voice operation.
MOS value	MOS value calculated for the voice operation.
ICPIF value	ICPIF value calculated for the voice operation.
Hop IP	IP address of the hop. This field is available only for the path jitter operation.
Path-jitter results	Path jitter operation results. This field is available only for the path jitter operation.
Jitter number	Number of jitters. This field is available only for the path jitter operation.
Min/Max/Average jitter	Minimum/maximum/average jitter in milliseconds. This field is available only for the path jitter operation.
Positive jitter number	Number of positive jitter. This field is available only for the path jitter operation.
Min/Max/Average positive jitter	Minimum/maximum/average positive jitter in milliseconds. This field is available only for the path jitter operation.
Sum/Square-Sum positive jitter	Sum/square sum of the positive jitter. This field is available only for the path jitter operation.
Negative jitter number	Number of negative jitter. This field is available only for the path jitter operation.
Min/Max/Average negative jitter	Minimum/maximum/average negative jitter in milliseconds. This field is available only for the path jitter operation.
Sum/Square-Sum negative jitter	Sum/square sum of the negative jitter. This field is available only for the path jitter operation.
TTL	If the routing table bypass feature is not enabled in the operation, this field displays the TTL value in the probe packet. If the routing table bypass feature is enabled, this field value varies by the **`init-ttl`** command. However, the actual TTL value in the probe packet is fixed at 1.
Hop IP	IP address of the node that sent the reply packet.
Time	Time when the NQA client received the reply packet.

display nqa statistics

Use **display nqa statistics** to display NQA operation statistics.

Syntax

display nqa statistics [*admin-name operation-tag*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

admin-name operation-tag: Specifies an NQA operation by its administrator name and operation tag. The *admin-name* argument represents the name of the administrator who creates the NQA operation. The *operation-tag* argument represents the operation tag. Each of the arguments is a case-insensitive string of 1 to 32 characters that cannot contain hyphens (-). If you do not specify an NQA operation, the command displays statistics for all NQA operations.

Usage guidelines

The statistics are generated after the NQA operation completes. If you execute the **display nqa statistics** command before the operation completes, the statistics are displayed as all 0s.

If a reaction entry is configured, the command displays the monitoring results of the reaction entry in the period specified by the **statistics internal** command. The result fields display hyphens (-) in one of the following conditions:

- The threshold type is average value.
- The monitored performance metric is ICPIF or MOS for the voice operation.

Examples

Display the statistics for the TCP operation with administrator name **admin** and operation tag **test**.

```
<Sysname> display nqa statistics admin test
NQA entry (admin admin, tag test) test statistics:
  NO. : 1
    Start time: 2007-01-01 09:30:20.0
    Life time: 2 seconds
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 13/13/13
    Square-Sum of round trip time: 169
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to disconnect: 0
    Failures due to no connection: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

Display the statistics for the ICMP jitter operation with administrator name **admin** and operation tag **test**.

```
<Sysname> display nqa statistics admin test
NQA entry (admin admin, tag test) test statistics:
```

```
  NO. : 1
    Start time: 2015-03-09 17:42:10.7
    Life time: 156 seconds
    Send operation times: 1560           Receive response times: 1560
    Min/Max/Average round trip time: 1/2/1
    Square-Sum of round trip time: 1563
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
  ICMP-jitter results:
   RTT number: 1560
    Min positive SD: 1                   Min positive DS: 1
    Max positive SD: 1                   Max positive DS: 2
    Positive SD number: 18               Positive DS number: 46
    Positive SD sum: 18                  Positive DS sum: 49
    Positive SD average: 1               Positive DS average: 1
    Positive SD square-sum: 18           Positive DS square-sum: 55
    Min negative SD: 1                   Min negative DS: 1
    Max negative SD: 1                   Max negative DS: 2
    Negative SD number: 24               Negative DS number: 57
    Negative SD sum: 24                  Negative DS sum: 58
    Negative SD average: 1               Negative DS average: 1
    Negative SD square-sum: 24           Negative DS square-sum: 60
    SD average: 1                        DS average: 1
  One way results:
    Max SD delay: 1                      Max DS delay: 2
    Min SD delay: 1                      Min DS delay: 1
    Number of SD delay: 4                Number of DS delay: 4
    Sum of SD delay: 4                   Sum of DS delay: 5
    Square-Sum of SD delay: 4            Square-Sum of DS delay: 7
    Lost packets for unknown reason: 0
  Reaction statistics:
    Index  Checked Element  Threshold Type  Checked Num  Over-threshold Num
    1      jitter-DS        accumulate      1500         10
    2      jitter-SD        average         -            -
    3      OWD-DS           -               1560         2
    4      OWD-SD           -               1560         0
    5      packet-loss      accumulate      0            0
    6      RTT              accumulate      1560         0
```

Display the statistics for the UDP jitter operation with administrator name **admin** and operation tag **test**.

```
<Sysname> display nqa statistics admin test
NQA entry (admin admin, tag test) test statistics:
  NO. : 1
```

```
    Start time: 2007-01-01 09:33:22.3
    Life time: 23 seconds
    Send operation times: 100            Receive response times: 100
    Min/Max/Average round trip time: 1/11/5
    Square-Sum of round trip time: 24360
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
  UDP-jitter results:
   RTT number: 550
    Min positive SD: 1                   Min positive DS: 1
    Max positive SD: 7                   Max positive DS: 1
    Positive SD number: 220              Positive DS number: 97
    Positive SD sum: 283                 Positive DS sum: 287
    Positive SD average: 1               Positive DS average: 2
    Positive SD square-sum: 709          Positive DS square-sum: 1937
    Min negative SD: 2                   Min negative DS: 1
    Max negative SD: 10                  Max negative DS: 1
    Negative SD number: 81               Negative DS number: 94
    Negative SD sum: 556                 Negative DS sum: 191
    Negative SD average: 6               Negative DS average: 2
    Negative SD square-sum: 4292         Negative DS square-sum: 967
    SD average: 2                        DS average: 2
  One way results:
    Max SD delay: 5                      Max DS delay: 5
    Min SD delay: 1                      Min DS delay: 1
    Number of SD delay: 550              Number of DS delay: 550
    Sum of SD delay: 1475                Sum of DS delay: 1201
    Square-Sum of SD delay: 5407         Square-Sum of DS delay: 3959
    SD lost packets: 0                   DS lost packets: 0
    Lost packets for unknown reason: 0
  Reaction statistics:
    Index  Checked Element  Threshold Type  Checked Num  Over-threshold Num
    1      jitter-DS        accumulate      90           25
    2      jitter-SD        average         -            -
    3      OWD-DS           -               100          24
    4      OWD-SD           -               100          13
    5      packet-loss      accumulate      0            0
    6      RTT              accumulate      100          52
```

Display the statistics for the voice operation with administrator name **admin** and operation tag **test**.

```
<Sysname> display nqa statistics admin test
NQA entry (admin admin, tag test) test statistics:
  NO. : 1
    Start time: 2007-01-01 09:33:45.3
```

```
    Life time: 120 seconds
    Send operation times: 10             Receive response times: 10
    Min/Max/Average round trip time: 1/12/7
    Square-Sum of round trip time: 620
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
  Voice results:
   RTT number: 10
    Min positive SD: 3                   Min positive DS: 1
    Max positive SD: 10                  Max positive DS: 1
    Positive SD number: 3                Positive DS number: 2
    Positive SD sum: 18                  Positive DS sum: 2
    Positive SD average: 6               Positive DS average: 1
    Positive SD square-sum: 134          Positive DS square-sum: 2
    Min negative SD: 3                   Min negative DS: 1
    Max negative SD: 9                   Max negative DS: 1
    Negative SD number: 4                Negative DS number: 2
    Negative SD sum: 25                  Negative DS sum: 2
    Negative SD average: 6               Negative DS average: 1
    Negative SD square-sum: 187          Negative DS square-sum: 2
    SD average: 6                        DS average: 1
  One way results:
    Max SD delay: 0                      Max DS delay: 0
    Min SD delay: 0                      Min DS delay: 0
    Number of SD delay: 0                Number of DS delay: 0
    Sum of SD delay: 0                   Sum of DS delay: 0
    Square-Sum of SD delay: 0            Square-Sum of DS delay: 0
    SD lost packets: 0                   DS lost packets: 0
    Lost packets for unknown reason: 0
  Voice scores:
    Max MOS value: 4.40                  Min MOS value: 4.40
    Max ICPIF value: 0                   Min ICPIF value: 0
  Reaction statistics:
    Index  Checked Element  Threshold Type  Checked Num  Over-threshold Num
    1      ICPIF            -               -            -
    2      MOS              -               -            -
```

Display the statistics for the path jitter operation with administrator name **admin** and operation tag **test**.

```
<Sysname> display nqa statistics admin test
NQA entry (admin admin, tag test) test statistics:
  NO. : 1
  Path 1:
  Hop IP 192.168.40.210
```

```
  Basic Results:
    Send operation times: 10
    Receive response times: 10
    Min/Max/Average round trip time: 1/1/1
    Square-Sum of round trip time: 10
  Extended Results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
  Path-Jitter Results:
    Jitter number: 9
      Min/Max/Average jitter: 0/0/0
    Positive jitter number: 0
      Min/Max/Average positive jitter: 0/0/0
      Sum/Square-Sum positive jitter: 0/0
    Negative jitter number: 0
      Min/Max/Average negative jitter: 0/0/0
      Sum/Square-Sum negative jitter: 0/0
Hop IP 192.168.50.209
  Basic Results:
    Send operation times: 10
    Receive response times: 10
    Min/Max/Average round trip time: 1/1/1
    Square-Sum of round trip time: 10
  Extended Results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
  Path-Jitter Results:
    Jitter number: 9
      Min/Max/Average jitter: 0/0/0
    Positive jitter number: 0
      Min/Max/Average positive jitter: 0/0/0
      Sum/Square-Sum positive jitter: 0/0
    Negative jitter number: 0
      Min/Max/Average negative jitter: 0/0/0
      Sum/Square-Sum negative jitter: 0/0
```

Table 7 Command output

Field	Description
No.	Statistics group ID.
Start time	Time when the operation started.

Field	Description
Life time	Duration of the operation in seconds.
Send operation times	Number of probe packets sent.
Receive response times	Number of response packets received.
Min/Max/Average round trip time	Minimum/maximum/average round-trip time in milliseconds.
Square-Sum of round trip time	Square sum of round-trip time.
Packet loss ratio	Average packet loss ratio.
Failures due to timeout	Number of timeout occurrences in an operation.
Failures due to disconnect	Number of disconnections by the peer.
Failures due to no connection	Number of failures to connect with the peer.
Failures due to internal error	Number of failures due to internal errors.
Failures due to other errors	Failures due to other errors.
Packets out of sequence	Number of failures due to out-of-sequence packets.
Packets arrived late	Number of response packets received after a probe times out.
ICMP-jitter results	ICMP jitter operation results. This field is available only for the ICMP jitter operation.
UDP-jitter results	UDP jitter operation results. This field is available only for the UDP jitter operation.
Voice results	Voice operation results. This field is available only for the voice operation.
RTT number	Number of response packets received.
Min positive SD	Minimum positive jitter from source to destination.
Min positive DS	Minimum positive jitter from destination to source.
Max positive SD	Maximum positive jitter from source to destination.
Max positive DS	Maximum positive jitter from destination to source.
Positive SD number	Number of positive jitters from source to destination.
Positive DS number	Number of positive jitters from destination to source.
Positive SD sum	Sum of positive jitters from source to destination.
Positive DS sum	Sum of positive jitters from destination to source.
Positive SD average	Average positive jitters from source to destination.
Positive DS average	Average positive jitters from destination to source.
Positive SD square-sum	Square sum of positive jitters from source to destination.
Positive DS square-sum	Square sum of positive jitters from destination to source.
Min negative SD	Minimum absolute value among negative jitters from source to destination.

Field	Description
Min negative DS	Minimum absolute value among negative jitters from destination to source.
Max negative SD	Maximum absolute value among negative jitters from source to destination.
Max negative DS	Maximum absolute value among negative jitters from destination to source.
Negative SD number	Number of negative jitters from source to destination.
Negative DS number	Number of negative jitters from destination to source.
Negative SD sum	Sum of absolute values of negative jitters from source to destination.
Negative DS sum	Sum of absolute values of negative jitters from destination to source.
Negative SD average	Average absolute value of negative jitters from source to destination.
Negative DS average	Average absolute value of negative jitters from destination to source.
Negative SD square-sum	Square sum of negative jitters from source to destination.
Negative DS square-sum	Square sum of negative jitters from destination to source.
SD average	Average value of jitters from source to destination.
DS average	Average value of jitters from destination to source.
One way results	Unidirectional delay result. This field is available only for the ICMP jitter, UDP jitter, and voice operations.
Max SD delay	Maximum delay from source to destination.
Max DS delay	Maximum delay from destination to source.
Min SD delay	Minimum delay from source to destination.
Min DS delay	Minimum delay from destination to source.
Number of SD delay	Number of delays from source to destination.
Number of DS delay	Number of delays from destination to source.
Sum of SD delay	Sum of delays from source to destination.
Sum of DS delay	Sum of delays from destination to source.
Square-Sum of SD delay	Square sum of delays from source to destination.
Square-Sum of DS delay	Square sum of delays from destination to source.
SD lost packets	Number of lost packets from the source to the destination.
DS lost packets	Number of lost packets from the destination to the source.
Lost packets for unknown reason	Number of lost packets for unknown reasons.

Field	Description
Voice scores	Voice parameters. This field is available only for the voice operation.
Max MOS value	Maximum MOS value.
Min MOS value	Minimum MOS value.
Max ICPIF value	Maximum ICPIF value.
Min ICPIF value	Minimum ICPIF value.
Reaction statistics	Statistics about the reaction entry in the counting interval.
Index	ID of a reaction entry.
Checked Element	Monitored element.
Threshold Type	Threshold type.
Checked Num	Number of targets that have been monitored for data collection.
Over-threshold Num	Number of threshold violations.
Path	Serial number for the path in the path jitter operation. This field is available only for the path jitter operation.
Hop IP	IP address of the hop. This field is available only for the path jitter operation.
Path-jitter results	Path jitter operation results. This field is available only for the path jitter operation.
Jitter number	Number of jitters. This field is available only for the path jitter operation.
Min/Max/Average jitter	Minimum/maximum/average positive jitter in milliseconds. This field is available only for the path jitter operation.
Positive jitter number	Number of positive jitters. This field is available only for the path jitter operation.
Min/Max/Average positive jitter	Minimum/maximum/average positive jitter in milliseconds. This field is available only for the path jitter operation.
Sum/Square-Sum positive jitter	Sum/square sum of positive jitters. This field is available only for the path jitter operation.
Negative jitter number	Number of negative jitters. This field is available only for the path jitter operation.
Min/Max/Average negative jitter	Minimum/maximum/average negative jitter in milliseconds. This field is available only for the path jitter operation.
Sum/Square-Sum negative jitter	Sum/square sum of negative jitters. This field is available only for the path jitter operation.

Table 8 Monitored performance metrics for DHCP/DLSw/DNS/FTP/HTTP/ICMP echo/SNMP/TCP/UDP echo operations

Monitored performance metric	Threshold type	Collect data in	Checked Num	Over-threshold Num
probe-duration	accumulate	Probes in the counting interval.	Number of completed probes.	Number of probes of which the duration exceeds the threshold.
	average	N/A	N/A	N/A
	consecutive	Probes in the counting interval.	Number of completed probes.	Number of probes of which the duration exceeds the threshold.
probe-fail	accumulate	Probes in the counting interval.	Number of completed probes.	Number of probe failures.
	consecutive	Probes in the counting interval.	Number of completed probes.	Number of probe failures.

Table 9 Monitored performance metrics for ICMP jitter/UDP jitter/voice operations

Monitored performance metric	Threshold type	Collect data in	Checked Num	Over-threshold Num
RTT	accumulate	Packets sent in the counting interval.	Number of sent packets.	Number of packets of which the round-trip time exceeds the threshold.
	average	N/A	N/A	N/A
jitter-DS/jitter-SD	accumulate	Packets sent in the counting interval.	Number of sent packets.	Number of packets of which the one-way jitter exceeds the threshold.
	average	N/A	N/A	N/A
OWD-DS/OWD-SD	N/A	Packets sent in the counting interval.	Number of sent packets.	Number of packets of which the one-way delay exceeds the threshold.
packet-loss	accumulate	Packets sent in the counting interval.	Number of sent packets.	Number of packet loss.
ICPIF/MOS (available only for the voice operation)	N/A	N/A	N/A	N/A

Related commands

`statistics interval`

expect data

Use **`expect data`** to configure the expected data.

Use **`undo expect data`** to restore the default.

Syntax

expect data *expression* [**offset** *number*]

undo expect data

Default

No expected data is configured.

Views

HTTP/HTTPS/TCP/UDP template view

Predefined user roles

network-admin

Parameters

expression: Specifies the expected data, a case-sensitive string of 1 to 200 characters.

offset *number*: Specifies the offset in bytes after which the first match operation starts. The value range for the *number* argument is 0 to 1000, and the default value is 0. If you do not specify an offset, the match operation starts from the beginning byte of the payload.

Usage guidelines

Upon receiving a response packet, the NQA client examines the target payload for the expected data.

- If a match is found, the NQA client verifies the NQA destination device as legal.
- If no match is found, the NQA client looks up the entire payload for a match. If no match is found again, the NQA destination device is verified as illegal. The NQA client does not perform the second round if no offset is specified. It verifies the NQA destination as illegal directly if no match is found for the first round.

Expected data check takes place in the following conditions:

- For features that use the HTTP or HTTPS template, the NQA client checks for the expected data if the response contains the Content-Length header.
- For features that use the TCP or UDP template, the NQA client checks for the expected data if the **data-fill** command is configured.

  The first five bytes of the UDP packet payload identify the probe packet type. The start byte of the offset is the sixth byte of the UDP payload.

Examples

In HTTP template view, set the expected data to **welcome!**.

```
<Sysname> system-view
[Sysname] nqa template http httptplt
[Sysname-nqatplt-http-httptplt] expect data welcome!
```

expect ip

Use **expect ip** to specify the expected IPv4 address.

Use **undo expect ip** to restore the default.

Syntax

expect ip *ip-address*

undo expect ip

Default

No expected IPv4 address is specified.

Views

DNS template view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the expected IPv4 address for a DNS echo request.

Usage guidelines

During a DNS operation, the NQA client compares the expected IPv4 address with the IPv4 address resolved by the DNS server. If they are the same, it considers the DNS server legal.

Examples

In DNS template view, specify 1.1.1.1 as the expected IPv4 address.

```
<Sysname> system-view
[Sysname] nqa template dns dnstplt
[Sysname-nqatplt-dns-dnstplt] expect ip 1.1.1.1
```

expect ipv6

Use **expect ipv6** to specify the expected IPv6 address.

Use **undo expect ipv6** to restore the default.

Syntax

expect ipv6 *ipv6-address*

undo expect ipv6

Default

No expected IPv6 address is specified.

Views

DNS template view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the expected IPv6 address for a DNS echo request.

Usage guidelines

During a DNS operation, the NQA client compares the expected IPv6 address with the IPv6 address resolved by the DNS server. If they are the same, it considers the DNS server legal.

Examples

In DNS template view, specify 1::1 as the expected IPv6 address.

```
<Sysname> system-view
[Sysname] nqa template dns dnstplt
[Sysname-nqatplt-dns-dnstplt] expect ipv6 1::1
```

expect status

Use **expect status** to configure the expected status code.

Use **undo expect status** to restore the default.

Syntax

expect status *status-list*

undo expect status [*status-list*]

Default

No expected status code is configured.

Views

HTTP template view

HTTPS template view

Predefined user roles

network-admin

Parameters

status-list: Specifies a space-separated list of up to 10 status code items. Each item specifies a status code or a range of status codes in the form of *status-num* 1 **to** *status-num 2*. The value ranges for both the *status-num* 1 and *status-num 2* arguments are 0 to 999. The value for the *status-num* 2 argument must be equal to or greater than the value for the *status-num* 1 argument.

Usage guidelines

The status code of the HTTP or HTTPS packet is a three-digit field in decimal notation, and the code includes the server status information. The first digit defines the class of response.

Examples

In HTTP template view, set the expected status codes to 200, 300, and 400 to 500.

```
<Sysname> system-view
[Sysname] nqa template http httptplt
[Sysname-nqatplt-http-httptplt] expect status 200 300 400 to 500
```

filename

Use **filename** to specify a file to be transferred between the FTP server and the FTP client.

Use **undo filename** to restore the default.

Syntax

filename *filename*

undo filename

Default

No file is specified.

Views

FTP operation view

FTP template view

Predefined user roles

network-admin

Parameters

filename: Specifies the name of a file, a case-sensitive string of 1 to 200 characters that cannot contain slashes (/).

Examples

Specify **config.txt** as the file to be transferred between the FTP server and the FTP client for the FTP operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp] filename config.txt
```

In FTP template view, specify **config.txt** as the file to be transferred between the FTP server and the FTP client.

```
<Sysname> system-view
[Sysname] nqa template ftp ftptplt
[Sysname-nqatplt-ftp-ftptplt] filename config.txt
```

frequency

Use **frequency** to specify the interval at which the NQA operation repeats.

Use **undo frequency** to restore the default.

Syntax

frequency *interval*

undo frequency

Default

In NQA operation view, the interval between two consecutive voice or path jitter operations is 60000 milliseconds. The interval between two consecutive operations of other types is 0 milliseconds.

In NQA template view, the interval between two consecutive operations is 5000 milliseconds.

Views

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP tracert operation view

ICMP jitter/path jitter/UDP jitter/voice operation view

Any NQA template view

Predefined user roles

network-admin

Parameters

interval: Specifies the interval between two consecutive operations, in the range of 0 to 604800000 milliseconds. An interval of 0 milliseconds configures NQA to perform the operation only once, and not to generate any statistics.

Usage guidelines

After an NQA operation starts, it repeats at the specified interval. However, when the interval is reached, but the current operation is not completed or not timed out, the next operation does not start.

Examples

Configure the ICMP echo operation to repeat every 1000 milliseconds.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] frequency 1000
```

In DNS template view, configure the DNS operation to repeat every 1000 milliseconds.

```
<Sysname> system-view
[Sysname] nqa template dns dnstplt
[Sysname-nqatplt-dns-dnstplt] frequency 1000
```

Related commands

probe timeout

history-record enable

Use **history-record enable** to enable the saving of history records for the NQA operation.

Use **undo history-record enable** to disable the saving of history records.

Syntax

history-record enable

undo history-record enable

Default

The saving of history records is enabled only for the UDP tracert operation.

Views

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP tracert operation view

Predefined user roles

network-admin

Usage guidelines

To display the history records of the NQA operation, use the **display nqa history** command.

The **undo** form of the command also removes existing history records of an NQA operation.

Examples

Enable the saving of history records for the NQA operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] history-record enable
```

Related commands

display nqa history

history-record keep-time

Use **history-record keep-time** to set the lifetime of history records for an NQA operation.

Use **undo history-record keep-time** to restore the default.

Syntax

history-record keep-time *keep-time*

undo history-record keep-time

Default

The history records of an NQA operation are kept for 120 minutes.

Views

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP tracert operation view

Predefined user roles

network-admin

Parameters

keep-time: Specifies how long the history records can be saved. The value range is 1 to 1440 minutes.

Usage guidelines

When an NQA operation completes, the timer starts. All records are removed when the lifetime is reached.

Examples

Set the lifetime of the history records to 100 minutes for the ICMP echo operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] history-record keep-time 100
```

history-record number

Use **history-record number** to set the maximum number of history records that can be saved for an NQA operation.

Use **undo history-record number** to restore the default.

Syntax

history-record number *number*

undo history-record number

Default

A maximum of 50 history records can be saved for an NQA operation.

Views

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP tracert operation view

Predefined user roles

network-admin

Parameters

number: Specifies the maximum number of history records that can be saved for an NQA operation. The value range is 0 to 50.

Usage guidelines

If the number of history records for an NQA operation exceeds the maximum number, earliest history records are removed.

Examples

Set the maximum number of history records to 10 for the ICMP echo operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] history-record number 10
```

init-ttl

Use **init-ttl** to set the TTL value for UDP packets in the start round of the UDP tracert operation.

Use **undo init-ttl** to restore the default.

Syntax

init-ttl *value*

undo init-ttl

Default

The NQA client sends a UDP packet with the TTL value 1 to start the UDP tracert operation.

Views

UDP tracert operation view

Predefined user roles

network-admin

Parameters

value: Specifies the TTL value in the range of 1 to 255.

Examples

Set the TTL value to 5 for the UDP packets in the start round.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-tracert
[Sysname-nqa-admin-test-udp-tracert] init-ttl 5
```

key

Use **key** to set the shared key for secure RADIUS authentication.

Use **undo key** to restore the default.

Syntax

key { **cipher** | **simple** } *string*

undo key

Default

No shared key is configured for secure RADIUS authentication.

Views

RADIUS template view

Predefined user roles

network-admin

Parameters

cipher: Specifies a key in encrypted form.

simple: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the shared key string. Its plaintext form is a case-sensitive string of 1 to 64 characters. Its encrypted form is a case-sensitive string of 1 to 117 characters.

Usage guidelines

Make sure the NQA client and the RADIUS server have the same shared key.

Examples

In RADIUS template view, set the shared key to **abc** in plain text for secure RADIUS authentication.

```
<Sysname> system-view
[Sysname] nqa template radius radiustplt
[Sysname-nqatplt-radius-radiustplt] key simple abc
```

lsr-path

Use **lsr-path** to specify a loose source routing (LSR) path.

Use **undo lsr-path** to restore the default.

Syntax

lsr-path *ip-address*&<1-8>

undo lsr-path

Default

No LSR path is configured.

Views

Path jitter operation view

Predefined user roles

network-admin

Parameters

ip-address&<1-8>: Specifies a space-separated list of up to eight IP addresses. Each IP address represents a hop on the path.

Usage guidelines

The path jitter operation first uses tracert to detect each hop to the destination. It then sends ICMP echo requests to measure the delay and jitters from the source to each node. If multiple routes exist between the source and destination, the operation uses the path specified by using **lsr-path** command.

Examples

Specify 10.1.1.20 and 10.1.2.10 as the hops on the LSR path for the path jitter operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type path-jitter
[Sysname-nqa-admin-test- path-jitter] lsr-path 10.1.1.20 10.1.2.10
```

max-failure

Use **max-failure** to set the maximum number of consecutive probe failures in a UDP tracert operation.

Use **undo max-failure** to restore the default.

Syntax

max-failure *times*

undo max-failure

Default

A UDP tracert operation stops and fails when it detects five consecutive probe failures.

Views

UDP tracert operation view

Predefined user roles

network-admin

Parameters

times: Specifies the maximum number in the range of 0 to 255. When this argument is set to 0 or 255, the UDP tracert operation does not stop when consecutive probe failures occur.

Usage guidelines

When a UDP tracert operation detects the maximum number of consecutive probe failures, the operation fails and stops probing the path.

Examples

Set the maximum number of consecutive probe failures to 20 in a UDP tracert operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-tracert
[Sysname-nqa-admin-test-udp-tracert] max-failure 20
```

mode

Use **mode** to set the data transmission mode for the FTP operation.

Use **undo mode** to restore the default.

Syntax

mode { **active** | **passive** }

undo mode

Default

The FTP operation uses the data transmission mode **active**.

Views

FTP operation view

FTP template view

Predefined user roles

network-admin

Parameters

active: Sets the data transmission mode to active. The FTP server initiates a connection request.

passive: Sets the data transmission mode to passive. The FTP client initiates a connection request.

Examples

Set the data transmission mode to **passive** for the FTP operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp] mode passive
```

In FTP template view, set the data transmission mode to **passive** for the FTP operation.

```
<Sysname> system-view
[Sysname] nqa template ftp ftptplt
[Sysname-nqatplt-ftp-ftptplt] mode passive
```

next-hop ip

Use **next-hop ip** to specify the next hop IPv4 address for probe packets.

Use **undo next-hop ip** to restore the default.

Syntax

next-hop ip *ip-address*

undo next-hop ip

Default

No next hop IPv4 address is specified for probe packets.

Views

ICMP echo operation view

ICMP/TCP half open template view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IPv4 address of the next hop.

Usage guidelines

If the next hop IPv4 address is not configured, the device searches the routing table to determine the next hop IPv4 address for the probe packets.

Examples

Specify 10.1.1.1 as the next hop IPv4 address for the ICMP echo operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] next-hop ip 10.1.1.1
```

next-hop ipv6

Use **next-hop ipv6** to specify the next hop IPv6 address for probe packets.

Use **undo next-hop ipv6** to restore the default.

Syntax

next-hop ipv6 *ipv6-address*

undo next-hop ipv6

Default

No next hop IPv6 address is specified for probe packets.

Views

ICMP echo operation view

ICMP/TCP half open template view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the IPv6 address of the next hop. IPv6 link-local addresses are not supported.

Usage guidelines

If the next hop IPv6 address is not configured, the device searches the routing table to determine the next hop IPv6 address for the probe packets.

Examples

Specify 10::1 as the next hop IPv6 address for the ICMP echo operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] next-hop ipv6 10::1
```

no-fragment enable

Use **no-fragment enable** to enable the no-fragmentation feature.

Use **undo no-fragment enable** to disable the no-fragmentation feature.

Syntax

no-fragment enable

undo no-fragment enable

Default

The no-fragmentation feature is disabled.

Views

UDP tracert operation view

Predefined user roles

network-admin

Usage guidelines

The no-fragmentation feature sets the DF field to 1. Packets with the DF field set cannot be fragmented during the forwarding process.

You can use this command to test the path MTU of a link.

Examples

Enable the no-fragmentation feature for the UDP tracert operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-tracert
[Sysname-nqa-admin-test-udp-tracert] no-fragment enable
```

nqa

Use **nqa** to create an NQA operation and enter its view, or enter the view of an existing NQA operation.

Use **undo nqa** to remove the operation.

Syntax

nqa entry *admin-name operation-tag*

undo nqa { **all** | **entry** *admin-name operation-tag* }

Default

No NQA operations exist.

Views

System view

Predefined user roles

network-admin

Parameters

admin-name operation-tag: Specifies an NQA operation by its administrator name and operation tag. The *admin-name* argument represents the name of the administrator who creates

the NQA operation. The *operation-tag* argument represents the operation tag. Each of the arguments is a case-insensitive string of 1 to 32 characters that cannot contain hyphens (-).

all: Removes all NQA operations.

Examples

Create an NQA operation with administrator name **admin** and operation tag **test**, and enter NQA operation view.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test]
```

nqa agent enable

Use **nqa agent enable** to enable the NQA client.

Use **undo nqa agent enable** to disable the NQA client and stop all operations being performed.

Syntax

nqa agent enable

undo nqa agent enable

Default

The NQA client is enabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable the NQA client.

```
<Sysname> system-view
[Sysname] nqa agent enable
```

Related commands

nqa server enable

nqa schedule

Use **nqa schedule** to configure scheduling parameters for an NQA operation.

Use **undo nqa schedule** to stop the operation.

Syntax

nqa schedule *admin-name operation-tag* **start-time** { *hh*:*mm*:*ss* [*yyyy/mm/dd* | *mm/dd/yyyy*] | **now** } **lifetime** { *lifetime* | **forever** } [**recurring**]

undo nqa schedule *admin-name operation-tag*

Default

No schedule is configured for an NQA operation.

Views

System view

Predefined user roles

network-admin

Parameters

admin-name operation-tag: Specifies an NQA operation by its administrator name and operation tag. The *admin-name* argument represents the name of the administrator who creates the NQA operation. The *operation-tag* argument represents the operation tag. Each of the arguments is a case-insensitive string of 1 to 32 characters that cannot contain hyphens (-).

start-time: Specifies the start time and date of the NQA operation.

hh:*mm*:*ss*: Specifies the start time of an NQA operation.

yyyy/mm/dd: Specifies the start date of an NQA operation. The default value is the current system time, and the value for the *yyyy* argument is in the range of 2000 to 2035.

mm/dd/yyyy: Specifies the start date of an NQA operation. The default value is the current system time, and the value for the *yyyy* argument is in the range of 2000 to 2035.

now: Starts the operation immediately.

lifetime: Specifies the duration of an operation.

lifetime: Specifies the duration of an operation in seconds. The value range is 1 to 2147483647.

forever: Performs the operation until you stop it by using the **undo nqa schedule** command.

recurring: Runs the operation automatically at the start time and for the specified duration. If you do not specify this keyword, the NQA operation is performed only once at the specified date and time.

Usage guidelines

The NQA operation works between the specified start time and the end time (the start time plus operation duration). If the specified start time is ahead of the system time, the operation starts immediately. If both the specified start time and end time are ahead of the system time, the operation does not start. To display the current system time, use the **display clock** command.

You cannot enter the view of a scheduled NQA operation. If you want to enter such view, use the **undo nqa schedule** command to stop the NQA operation first.

Examples

Schedule the operation with administrator name **admin** and operation tag **test** to start on 08:08:08 2008/08/08 and last 1000 seconds.

```
<Sysname> system-view
[Sysname] nqa schedule admin test start-time 08:08:08 2008/08/08 lifetime 1000 recurring
```

Related commands

destination ip

display clock (*Fundamentals Command Reference*)

nqa entry

type

nqa template

Use **nqa template** to create an NQA template and enter its view, or enter the view of an existing NQA template.

Use **undo nqa template** to remove an NQA template.

Syntax

nqa template { **dns** | **ftp** | **http** | **https** | **icmp** | **radius** | **ssl** | **tcp** | **tcphalfopen** | **udp** } *name*

undo nqa template { **dns** | **ftp** | **http** | **https** | **icmp** | **radius** | **ssl** | **tcp** | **tcphalfopen** | **udp** } *name*

Default

No NQA templates exist.

Views

System view

Predefined user roles

network-admin

Parameters

dns: Specifies the DNS template.

ftp: Specifies the FTP template.

http: Specifies the HTTP template.

https: Specifies the HTTPS template.

icmp: Specifies the ICMP template.

radius: Specifies the RADIUS template.

ssl: Specifies the SSL template.

tcp: Specifies the TCP template.

tcphalfopen: Specifies the TCP half open template.

udp: Specifies the UDP template.

name: Specifies the name of the NQA template, a case-insensitive string of 1 to 32 characters.

Examples

Create an ICMP template named **icmptplt**, and enter its view.

```
<Sysname> system-view
[Sysname] nqa template icmp icmptplt
[Sysname-nqatplt-icmp-icmptplt]
```

operation (FTP operation view)

Use **operation** to specify the operation type for the FTP operation.

Use **undo operation** to restore the default.

Syntax

operation { **get** | **put** }

undo operation

Default

The FTP operation type is **get**.

Views

FTP operation view

FTP template view

Predefined user roles

network-admin

Parameters

get: Gets a file from the FTP server.

put: Transfers a file to the FTP server.

Usage guidelines

When you perform the **put** operation with the **filename** command configured, make sure the file exists on the NQA client.

If you get a file from the FTP server, make sure the file specified in the URL exists on the FTP server. The NQA client does not save the file obtained from the FTP server.

Use a small file for the FTP operation. A big file might result in transfer failure because of timeout, or might affect other services for occupying much network bandwidth.

Examples

Set the operation type to **put** for the FTP operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp] operation put
```

In FTP template view, set the operation type to **put** for the FTP operation.

```
<Sysname> system-view
[Sysname] nqa template ftp ftptplt
[Sysname-nqatplt-ftp-ftptplt] operation put
```

Related commands

password

username

operation (HTTP/HTTPS operation view)

Use **operation** to specify the operation type for the HTTP or HTTPS operation.

Use **undo operation** to restore the default.

Syntax

operation { **get** | **post** | **raw** }

undo operation

Default

The HTTP or HTTPS operation type is **get**.

Views

HTTP operation view

HTTP/HTTPS template view

Predefined user roles

network-admin

Parameters

get: Gets data from the HTTP or HTTPS server.

post: Transfers data to the HTTP or HTTPS server.

raw: Sends the RAW request to the HTTP or HTTPS server.

Usage guidelines

The HTTP and HTTPS operations use HTTP and HTTPS requests as probe packets.

For the **get** or **post** operation, the content in the request is obtained from the URL specified by the **url** command.

For the **raw** operation, the content in the request is configured in raw request view. You can use the **raw-request** command to enter the raw request view.

Examples

Set the operation type to **raw** for the HTTP operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type http
[Sysname-nqa-admin-test-http] operation raw
```

In HTTP template view, set the operation type to **raw** for the HTTP operation.

```
<Sysname> system-view
[Sysname] nqa template http httptplt
[Sysname-nqatplt-http-httptplt] operation raw
```

Related commands

password

raw-request

username

out interface

Use **out interface** to specify the output interface for probe packets.

Use **undo out interface** to restore the default.

Syntax

out interface *interface-type interface-number*

undo out interface

Default

The output interface for probe packets is not specified. The NQA client determines the output interface based on the routing table lookup.

Views

ICMP echo operation view

DHCP operation view

UDP tracert operation view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

For successful operation, the specified output interface must be up.

If both the **next-hop** and **out interface** commands are configured for the ICMP echo operation, the **out interface** command does not take effect.

Examples

Specify VLAN-interface 1 as the output interface for probe packets in the UDP tracert operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-tracert
[Sysname-nqa-admin-test-udp-tracert] out interface vlan-interface 1
```

password

Use **password** to specify a password.

Use **undo password** to restore the default.

Syntax

password { **cipher** | **simple** } *string*

undo password

Default

No password is specified.

Views

FTP/HTTP operation view

FTP/HTTP/HTTPS/RADIUS template view

Predefined user roles

network-admin

Parameters

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. The value of the argument varies as follows:

- For FTP, HTTP, and HTTPS operations, the plaintext form of the password is a case-sensitive string of 1 to 32 characters. The encrypted form of the password is a case-sensitive string of 1 to 73 characters.
- For RADIUS templates, the plaintext form of the password is a case-sensitive string of 1 to 64 characters. The encrypted form of the password is a case-sensitive string of 1 to 117 characters.

Examples

Set the FTP login password to **ftpuser**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
```

```
[Sysname-nqa-admin-test-ftp] password simple ftpuser
```

Set the FTP login password to **ftpuser** in FTP template view.

```
<Sysname> system-view
[Sysname] nqa template ftp ftptplt
[Sysname-nqatplt-ftp-ftptplt] password simple ftpuser
```

Related commands

operation

username

probe count

Use **probe count** to specify the probe times.

Use **undo probe count** to restore the default.

Syntax

probe count *times*

undo probe count

Default

In an UDP tracert operation, the NQA client sends three probe packets to each hop along the path.

In other types of operations, the NQA client performs one probe to the destination per operation.

Views

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP tracert operation view

ICMP jitter/UDP jitter operation view

Predefined user roles

network-admin

Parameters

times: Specifies the probe times.

- For the UDP tracert operation, this argument specifies the times of probes to each hop along the path. The value range for this argument is 1 to 10.
- For other types of operations, this argument specifies the times of probes to the destination per operation. The value range for this argument is 1 to 15.

Usage guidelines

The following describes how NQA performs different types of operations:

- A TCP or DLSw operation sets up a connection.
- An ICMP jitter or UDP jitter operation sends a number of probe packets. The number of probe packets is set by using the **probe packet-number** command.
- An FTP operation uploads or downloads a file.
- An HTTP operation gets a Web page.
- A DHCP operation gets an IP address through DHCP.
- A DNS operation translates a domain name to an IP address.

- An ICMP echo sends an ICMP echo request.
- A UDP echo operation sends a UDP packet.
- An SNMP operation sends one SNMPv1 packet, one SNMPv2c packet, and one SNMPv3 packet.
- A UDP tracert operation determines the routing path from the source to the destination. The number of probe packets sent to each hop is set by using the **probe count** command.
- A frame loss, latency, or throughput operation sends probe frames to the destination device to test the frame loss ratio, latency, or throughput of the network.

If an operation is to perform multiple probes, the NQA client starts a new probe in one of the following conditions:

- The NQA client receives responses to packets sent in the last probe.
- The probe timeout time expires.

This command is not available for the voice or path jitter operations. Each of these operations performs only one probe.

Examples

Configure the ICMP echo operation to perform 10 probes.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] probe count 10
```

probe packet-interval

Use **probe packet-interval** to configure the packet sending interval in the probe.

Use **undo probe packet-interval** to restore the default.

Syntax

probe packet-interval *interval*

undo probe packet-interval

Default

The packet sending interval is 20 milliseconds.

Views

ICMP jitter/path jitter/UDP jitter/voice operation view

Predefined user roles

network-admin

Parameters

interval: Specifies the sending interval in the range of 10 to 60000 milliseconds.

Examples

Configure the UDP jitter operation to send packets every 100 milliseconds.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] probe packet-interval 100
```

probe packet-number

Use **probe packet-number** to set the number of packets to be sent in a UDP jitter, path jitter, or voice probe.

Use **undo probe packet-number** to restore the default.

Syntax

probe packet-number *packet-number*

undo probe packet-number

Default

An ICMP jitter, UDP jitter, or path jitter probe sends 10 packets and a voice probe sends 1000 packets.

Views

ICMP jitter/path jitter/UDP jitter/voice operation view

Predefined user roles

network-admin

Parameters

packet-number: Specifies the number of packets to be sent per probe. Available value ranges include:

- 10 to 1000 for the ICMP jitter, UDP jitter, and path jitter operations.
- 10 to 60000 for the voice operation.

Examples

Configure the UDP jitter probe to send 100 packets.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] probe packet-number 100
```

probe packet-timeout

Use **probe packet-timeout** to set the timeout time for waiting for a response in the UDP jitter, path jitter, or voice operation.

Use **undo probe packet-timeout** to restore the default.

Syntax

probe packet-timeout *timeout*

undo probe packet-timeout

Default

The response timeout time in the UDP jitter or path jitter operation is 3000 milliseconds.

The response timeout time in the voice operation is 5000 milliseconds.

Views

ICMP jitter/path jitter/UDP jitter/voice operation view

Predefined user roles

network-admin

Parameters

timeout: Specifies the timeout time in milliseconds. The value range is 10 to 3600000.

Examples

Set the response timeout time to 100 milliseconds in the UDP jitter operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] probe packet-timeout 100
```

probe timeout

Use **probe timeout** to set the probe timeout time.

Use **undo probe timeout** to restore the default.

Syntax

probe timeout *timeout*

undo probe timeout

Default

The timeout time of a probe is 3000 milliseconds.

Views

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP tracert operation view

Any NQA template view

Predefined user roles

network-admin

Parameters

timeout: Specifies the probe timeout time in milliseconds. The value range for this argument varies as follows:

- For FTP and HTTP operations, the value range is 10 to 86400000.
- For DHCP, DNS, DLSw, ICMP echo, SNMP, TCP, UDP echo, and UDP tracert operations, the value range is 10 to 3600000.
- For FTP, HTTP, and HTTPS templates, the value range is 10 to 86400000.
- For other types of NQA templates, the value range is 10 to 3600000.

Usage guidelines

If a probe does not complete within the period, the probe is timed out.

Examples

Set the probe timeout time to 10000 milliseconds for the DHCP operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
```

```
[Sysname-nqa-admin-test] type dhcp
[Sysname-nqa-admin-test-dhcp] probe timeout 10000
```

In HTTP template view, set the probe timeout time to 10000 milliseconds for the HTTP operation.

```
<Sysname> system-view
[Sysname] nqa template http httptplt
[Sysname-nqatplt-http-httptplt] probe timeout 10000
```

raw-request

Use **raw-request** to enter raw request view and specify the content of an HTTP or HTTPS request.

Use **undo raw-request** to restore the default.

Syntax

raw-request

undo raw-request

Default

The contents of an HTTP or HTTPS raw request are not specified.

Views

HTTP operation view

HTTP/HTTPS template view

Predefined user roles

network-admin

Usage guidelines

This command places you in raw request view and deletes the previously configured request content.

If the HTTP or HTTPS operation type is set to **raw**, you must enter raw request view and configure the request content to be sent to the HTTP or HTTPS server. To ensure successful operations, make sure the request content does not contain command aliases configured by using the **alias** command. For more information about the **alias** command, see CLI commands in *Fundamentals Command Reference*.

Examples

Enter raw request view and specify the content of a GET request for the HTTP operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type http
[Sysname-nqa-admin-test-http] raw-request
[Sysname-nqa-admin-test-http-raw-request] GET /sdn/ui/app/index HTTP/1.0\r\nHost:
172.0.0.2\r\n\r\n
```

In HTTP template view, enter raw request view and specify the content of a POST request for the HTTP operation.

```
<Sysname> system-view
[Sysname] nqa template http httptplt
[Sysname-nqatplt-http-httptplt] raw-request
[Sysname-nqatplt-http-httptplt-raw-request] POST /sdn/ui/app/index HTTP/1.0\r\nHost:
 172.0.0.2\r\nAuthorization: Basic cm9vdDoxMjM0NTY=\r\n\r\n
```

reaction checked-element { jitter-ds | jitter-sd }

Use **reaction checked-element** { **jitter-ds** | **jitter-sd** } to configure a reaction entry for monitoring one-way jitter in the NQA operation.

Use **undo reaction** to delete a reaction entry.

Syntax

reaction *item-number* **checked-element** { **jitter-ds** | **jitter-sd** } **threshold-type** { **accumulate** *accumulate-occurrences* | **average** } **threshold-value** *upper-threshold lower-threshold* [**action-type** { **none** | **trap-only** }]

undo reaction *item-number*

Default

No reaction entries for monitoring one-way jitter exist.

Views

ICMP jitter/UDP jitter/voice operation view

Predefined user roles

network-admin

Parameters

item-number: Assigns an ID to the reaction entry, in the range of 1 to 10.

jitter-ds: Specifies the destination-to-source jitter of each probe packet as the monitored element (or performance metric).

jitter-sd: Specifies source-to-destination jitter of each probe packet as the monitored element.

threshold-type: Specifies a threshold type.

accumulate *accumulate-occurrences*: Checks the total number of threshold violations in the operation. The value range is 1 to 14999 for the ICMP jitter and UDP jitter operations, and 1 to 59999 for the voice operation.

average: Checks the average one-way jitter.

threshold-value: Specifies threshold range in milliseconds.

upper-threshold: Specifies the upper limit in the range of 0 to 3600000.

lower-threshold: Specifies the lower limit in the range of 0 to 3600000. It must not be greater than the upper limit.

action-type: Specifies the action to be triggered. The default action is **none**.

none: Specifies the action of displaying results on the terminal display.

trap-only: Specifies the action of displaying results on the terminal display and meanwhile sending SNMP trap messages to the NMS.

Usage guidelines

You cannot edit a reaction entry after it is created. To change the attributes in a reaction entry, use the **undo reaction** command to delete the entry, and then configure a new one.

Only successful probe packets are monitored. Statistics about failed probe packets are not collected.

Examples

Create reaction entry 1 for monitoring the average destination-to-source jitter of UDP jitter packets, and set the upper limit to 50 milliseconds and the lower limit to 5 milliseconds. Before the NQA

operation starts, the initial state of the reaction entry is invalid. After the operation, the average destination-to-source jitter is checked against the threshold range. If it exceeds the upper limit, the state of the reaction entry is set to over-threshold. If it is below the lower limit, the state is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the NMS.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] reaction 1 checked-element jitter-ds threshold-type average threshold-value 50 5 action-type trap-only
```

Create reaction entry 2 for monitoring the destination-to-source jitter of UDP jitter probe packets, and set the upper limit to 50 milliseconds, and the lower limit to 5 milliseconds. Before the NQA operation starts, the initial state of the reaction entry is invalid. After the operation, the destination-to-source jitter is checked against the threshold range. If the total number of threshold violations reaches or exceeds 100, the state of the entry is set to over-threshold. Otherwise, the state of the entry is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the NMS.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] reaction 2 checked-element jitter-ds threshold-type accumulate 100 threshold-value 50 5 action-type trap-only
```

reaction checked-element { owd-ds | owd-sd }

Use **reaction checked-element** { **owd-ds** | **owd-sd** } to configure a reaction entry for monitoring the one-way delay.

Use **undo reaction** to delete a reaction entry.

Syntax

reaction *item-number* **checked-element** { **owd-ds** | **owd-sd** } **threshold-value** *upper-threshold lower-threshold*

undo reaction *item-number*

Default

No reaction entries for monitoring the one-way delay exist.

Views

ICMP jitter/UDP jitter/voice operation view

Predefined user roles

network-admin

Parameters

item-number: Assigns an ID to the reaction entry, in the range of 1 to 10.

owd-ds: Specifies the destination-to-source delay of each probe packet as the monitored element.

owd-sd: Specifies the source-to-destination delay of each probe packet as the monitored element.

threshold-value: Specifies threshold range in milliseconds.

upper-threshold: Specifies the upper limit in the range of 0 to 3600000.

lower-threshold: Specifies the lower limit in the range of 0 to 3600000. It must not be greater than the upper limit.

Usage guidelines

You cannot edit a reaction entry after it is created. To change the attributes in a reaction entry, use the **undo reaction** command to delete the entry, and then configure a new one.

Only successful probe packets are monitored. Statistics about failed probe packets are not collected.

No actions can be configured for a reaction entry of monitoring one-way delays. To display the monitoring results and statistics, use the **display nqa reaction counters** and **display nqa statistics** commands.

Examples

Create reaction entry 1 for monitoring the destination-to-source delay of every UDP jitter packet, and set the upper limit to 50 milliseconds and lower limit to 5 milliseconds. Before the NQA operation starts, the initial state of the reaction entry is invalid. The destination-to-source delay is calculated after the response to the probe packet arrives. If the delay exceeds the upper limit, the state of the reaction entry is set to over-threshold. If it is below the lower limit, the state is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the NMS.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] reaction 1 checked-element owd-ds threshold-value 50
5
```

reaction checked-element icpif

Use **reaction checked-element icpif** to configure a reaction entry for monitoring the ICPIF value in the voice operation.

Use **undo reaction** to delete a reaction entry.

Syntax

reaction *item-number* **checked-element icpif threshold-value** *upper-threshold lower-threshold* [**action-type** { **none** | **trap-only** }]

undo reaction *item-number*

Default

No reaction entries for monitoring ICPIF values exist.

Views

Voice operation view

Predefined user roles

network-admin

Parameters

item-number: Assigns an ID to the reaction entry, in the range of 1 to 10.

threshold-value: Specifies threshold range.

upper-threshold: Specifies the upper limit in the range of 1 to 100.

lower-threshold: Specifies the lower limit in the range of 1 to 100. It must not be greater than the upper limit.

action-type: Specifies what action to be triggered. The default action is **none**.

none: Specifies the action of displaying results on the terminal display.

trap-only: Specifies the action of displaying results on the terminal display and meanwhile sending SNMP trap messages to the NMS.

Usage guidelines

You cannot edit a reaction entry after it is created. To change the attributes in a reaction entry, use the **undo reaction** command to delete the entry, and then configure a new one.

Examples

Create reaction entry 1 for monitoring the ICPIF value in the voice operation, and set the upper limit to 50 and lower limit to 5. Before the voice operation starts, the initial state of the reaction entry is invalid. After the operation, the ICPIF value is checked against the threshold range. If it exceeds the upper limit, the state of the reaction entry is set to over-threshold. If it is below the lower limit, the state is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the NMS.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type voice
[Sysname-nqa-admin-test-voice] reaction 1 checked-element icpif threshold-value 50 5
action-type trap-only
```

reaction checked-element mos

Use **reaction checked-element mos** to configure a reaction entry for monitoring the MOS value in the voice operation.

Use **undo reaction** to delete a reaction entry.

Syntax

reaction *item-number* **checked-element mos threshold-value** *upper-threshold lower-threshold* [**action-type** { **none** | **trap-only** }]

undo reaction *item-number*

Default

No reaction entries for monitoring the MOS value exist.

Views

Voice operation view

Predefined user roles

network-admin

Parameters

item-number: Assigns an ID to the reaction entry, in the range of 1 to 10.

threshold-value: Specifies threshold range.

upper-threshold: Specifies the upper limit in the range of 1 to 500.

lower-threshold: Specifies the lower limit in the range of 1 to 500. It must not be greater than the upper limit.

action-type: Specifies what action to be triggered. The default action is **none**.

none: Specifies the action of displaying results on the terminal display.

trap-only: Specifies the action of displaying results on the terminal display and meanwhile sending SNMP trap messages to the NMS.

Usage guidelines

You cannot edit a reaction entry after it is created. To change the attributes in a reaction entry, use the **undo reaction** command to delete the entry, and then configure a new one.

For the MOS threshold, the number is expressed in three digits representing ones, tenths, and hundredths. For example, to express a MOS threshold of 1, enter 100.

Examples

Create reaction entry 1 for monitoring the MOS value of the voice operation, and set the upper limit to 2 and lower limit to 1. Before the NQA operation starts, the initial state of the reaction entry is invalid. After the operation, the MOS value is checked against the threshold range. If it exceeds the upper limit, the state of the reaction entry is set to over-threshold. If it is below the lower limit, the state is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the NMS.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type voice
[Sysname-nqa-admin-test-voice] reaction 1 checked-element mos threshold-value 200 100
action-type trap-only
```

reaction checked-element packet-loss

Use **reaction checked-element packet-loss** to configure a reaction entry for monitoring packet loss in UDP jitter or voice operation.

Use **undo reaction** to delete a reaction entry.

Syntax

reaction *item-number* **checked-element packet-loss threshold-type accumulate** *accumulate-occurrences* [**action-type** { **none** | **trap-only** }]

undo reaction *item-number*

Default

No reaction entries for monitoring packet loss exist.

Views

ICMP jitter/UDP jitter/voice operation view

Predefined user roles

network-admin

Parameters

item-number: Assigns an ID to the reaction entry, in the range of 1 to 10.

threshold-type: Specifies a threshold type.

accumulate *accumulate-occurrences*: Specifies the total number of lost packets in the operation. The value range is 1 to 15000 for the ICMP jitter and UDP jitter operations and 1 to 60000 for the voice operation.

action-type: Specifies what action to be triggered. The default action is **none**.

none: Specifies the action of displaying results on the terminal display.

trap-only: Specifies the action of displaying results on the terminal display and meanwhile sending SNMP trap messages to the NMS.

Usage guidelines

You cannot edit a reaction entry after it is created. To change the attributes in a reaction entry, use the **undo reaction** command to delete the entry, and then configure a new one.

Examples

Create reaction entry 1 for monitoring packet loss in the UDP jitter operation. Before the NQA operation starts, the initial state of the reaction entry is invalid. After the operation, the total number of the lost packets is checked against the threshold. If the number reaches or exceeds 100, the state of the reaction entry is set to over-threshold. Otherwise, the state is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the NMS.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] reaction 1 checked-element packet-loss
threshold-type accumulate 100 action-type trap-only
```

reaction checked-element probe-duration

Use **reaction checked-element probe-duration** to configure a reaction entry for monitoring the probe duration.

Use **undo reaction** to delete a reaction entry.

Syntax

reaction *item-number* **checked-element probe-duration threshold-type** { **accumulate** *accumulate-occurrences* | **average** | **consecutive** *consecutive-occurrences* } **threshold-value** *upper-threshold lower-threshold* [**action-type** { **none** | **trap-only** }]

undo reaction *item-number*

Default

No reaction entries for monitoring the probe duration exist.

Views

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

Predefined user roles

network-admin

Parameters

item-number: Assigns an ID to the reaction entry, in the range of 1 to 10.

threshold-type: Specifies a threshold type.

accumulate *accumulate-occurrences*: Checks the total number of threshold violations. The value range is 1 to 15.

average: Checks the average probe duration.

consecutive *consecutive-occurrences*: Specifies the number of consecutive threshold violations after the NQA operation starts. The value range is 1 to 16.

threshold-value: Specifies threshold range in milliseconds.

upper-threshold: Specifies the upper limit in the range of 0 to 3600000.

lower-threshold: Specifies the lower limit in the range of 0 to 3600000. It must not be greater than the upper threshold.

action-type: Specifies what action to be triggered. The default action is **none**.

none: Specifies the action of displaying results on the terminal display.

trap-only: Specifies the action of displaying results on the terminal display and meanwhile sending SNMP trap messages to the NMS. This keyword is not available for the DNS operation.

Usage guidelines

You cannot edit a reaction entry after it is created. To change the attributes in a reaction entry, use the **undo reaction** command to delete the entry, and then configure a new one.

Only successful probe packets are monitored. Statistics about failed probe packets are not collected.

Examples

Create reaction entry 1 for monitoring the average probe duration of ICMP echo operation, and set the upper limit to 50 milliseconds and lower limit to 5 milliseconds. Before the NQA operation starts, the initial state of the reaction entry is invalid. After the operation, the average probe duration is checked. If it exceeds the upper limit, the state is set to over-threshold. If it is below the lower limit, the state of the reaction entry is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the NMS.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-duration
threshold-type average threshold-value 50 5 action-type trap-only
```

Create reaction entry 2 for monitoring the probe duration of ICMP echo operation, and set the upper limit to 50 milliseconds and the lower limit to 5 milliseconds. Before the NQA operation starts, the initial state of the reaction entry is invalid. After the operation, the accumulated probe duration is checked against the threshold range. If the total number of threshold violations reaches or exceeds 10, the state of the entry is set to over-threshold. If it is below the lower threshold, the state of the entry is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the NMS.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] reaction 2 checked-element probe-duration
threshold-type accumulate 10 threshold-value 50 5 action-type trap-only
```

Create reaction entry 3 for monitoring the probe duration time of ICMP echo operation, and set the upper limit to 50 milliseconds and the lower limit to 5 milliseconds. Before the NQA operation starts, the initial state of the reaction entry is invalid. After the operation, the consecutive probe duration is checked against the threshold range. If the total number of consecutive threshold violations reaches or exceeds 10, the state of the entry is set to over-threshold. If it is below the lower threshold, the state of the entry is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the NMS.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] reaction 3 checked-element probe-duration
threshold-type consecutive 10 threshold-value 50 5 action-type trap-only
```

reaction checked-element probe-fail (for trap)

Use **reaction checked-element probe-fail** to configure a reaction entry for monitoring the probe failures of the operation.

Use **undo reaction** to delete a reaction entry.

Syntax

reaction *item-number* **checked-element probe-fail threshold-type** { **accumulate** *accumulate-occurrences* | **consecutive** *consecutive-occurrences* } [**action-type** { **none** | **trap-only** }]

undo reaction *item-number*

Default

No reaction entries for monitoring probe failures exist.

Views

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

Predefined user roles

network-admin

Parameters

item-number: Assigns an ID to the reaction entry, in the range of 1 to 10.

threshold-type: Specifies a threshold type.

accumulate *accumulate-occurrences*: Checks the total number of probe failures. The value range is 1 to 15.

consecutive *consecutive-occurrences*: Checks the maximum number of consecutive probe failures. The value range is 1 to 16.

action-type: Specifies what action to be triggered. The default action is **none**.

none: Specifies the action of displaying results on the terminal display.

trap-only: Specifies the action of displaying results on the terminal display and meanwhile sending SNMP trap messages to the NMS. This keyword is not available for the DNS operation.

Usage guidelines

You cannot edit a reaction entry after it is created. To change the attributes in a reaction entry, use the **undo reaction** command to delete the entry, and then configure a new one.

Examples

Create reaction entry 1 for monitoring the probe failures in ICMP echo operation. Before the NQA operation starts, the initial state of the reaction entry is invalid. If the total number of probe failures reaches or exceeds 10, the state of the entry is set to over-threshold. If it is below the threshold, the state of the entry is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the NMS.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail threshold-type
accumulate 10 action-type trap-only
```

Create reaction entry 2 for monitoring the probe failures in ICMP echo operation. Before the NQA operation starts, the initial state of the reaction entry is invalid. If the number of consecutive probe failures reaches or exceeds 10, the state of the entry is set to over-threshold. If it is below the threshold, the state of the entry is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the NMS.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] reaction 2 checked-element probe-fail threshold-type consecutive 10 action-type trap-only
```

reaction checked-element probe-fail (for trigger)

Use **reaction checked-element probe-fail** to configure a reaction entry for monitoring probe failures.

Use **undo reaction** to delete a reaction entry.

Syntax

reaction *item-number* **checked-element probe-fail threshold-type consecutive** *consecutive-occurrences* **action-type trigger-only**

undo reaction *item-number*

Default

No reaction entries for monitoring probe failures exist.

Views

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

Predefined user roles

network-admin

Parameters

item-number: Assigns an ID to the reaction entry, in the range of 1 to 10.

threshold-type: Specifies a threshold type.

consecutive *consecutive-occurrences*: Checks the maximum number of consecutive probe failures, in the range of 1 to 16.

action-type: Specifies what action to be triggered.

trigger-only: Triggers other modules to react to certain conditions.

Usage guidelines

You cannot edit a reaction entry after it is created. To change the attributes in a reaction entry, use the **undo reaction** command to delete the entry, and then configure a new one.

Examples

Create reaction entry 1. If the number of consecutive probe failures reaches 3, collaboration is triggered.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type tcp
```

```
[Sysname-nqa-admin-test-tcp] reaction 1 checked-element probe-fail threshold-type
consecutive 3 action-type trigger-only
```

Related commands

track (*High Availability Command Reference*)

reaction checked-element rtt

Use **reaction checked-element rtt** to configure a reaction entry for monitoring packet round-trip time.

Use **undo reaction** to delete a reaction entry.

Syntax

reaction *item-number* **checked-element rtt threshold-type** { **accumulate** *accumulate-occurrences* | **average** } **threshold-value** *upper-threshold lower-threshold* [**action-type** { **none** | **trap-only** }]

undo reaction *item-number*

Default

No reaction entries for monitoring packet round-trip time exist.

Views

ICMP jitter/UDP jitter/voice operation view

Predefined user roles

network-admin

Parameters

item-number: Assigns an ID to the reaction entry, in the range of 1 to 10.

threshold-type: Specifies a threshold type.

accumulate *accumulate-occurrences*: Checks the total number of threshold violations. Available value ranges include:

- 1 to 15000 for the ICMP jitter and UDP jitter operations.
- 1 to 60000 for the voice operation.

average: Checks the packet average round-trip time.

threshold-value: Specifies threshold range in milliseconds.

upper-threshold: Specifies the upper limit in the range of 0 to 3600000.

lower-threshold: Specifies the lower limit in the range of 0 to 3600000. It must not be greater than the upper limit.

action-type: Specifies what action to be triggered. The default action is **none**.

none: Specifies the action of displaying results on the terminal display.

trap-only: Specifies the action of displaying results on the terminal display and meanwhile sending SNMP trap messages to the NMS.

Usage guidelines

You cannot edit a reaction entry after it is created. To change the attributes in a reaction entry, use the **undo reaction** command to delete the entry, and then configure a new one.

Only successful probe packets are monitored. Statistics about failed probe packets are not collected.

Examples

Create reaction entry 1 for monitoring the average round-trip time of UDP jitter probe packets, and set the upper limit to 50 milliseconds and lower limit to 5 milliseconds. Before the NQA operation starts, the initial state of the reaction entry is invalid. After the operation, the average packet round-trip time is checked. If it exceeds the upper limit, the state is set to over-threshold. If it is below the lower limit, the state is set to below-threshold. Once the reaction entry state changes, a trap message is generated and sent to the NMS.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] reaction 1 checked-element rtt threshold-type
average threshold-value 50 5 action-type trap-only
```

Create reaction entry 2 for monitoring the round-trip time of UDP jitter probe packets, and set the upper limit to 50 milliseconds and lower limit to 5 milliseconds. Before the NQA operation starts, the initial state of the reaction entry is invalid. After the operation, the packet round-trip time is checked. If the total number of threshold violations reaches or exceeds 100, the state of the entry is set to over-threshold. Otherwise, the state of the entry is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the NMS.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] reaction 1 checked-element rtt threshold-type
accumulate 100 threshold-value 50 5 action-type trap-only
```

reaction trap

Use **reaction trap** to configure the sending of traps to the NMS under specific conditions.

Use **undo reaction trap** to restore the default.

Syntax

reaction trap { **path-change** | **probe-failure** *consecutive-probe-failures* | **test-complete** | **test-failure** [*accumulate-probe-failures*] }

undo reaction trap { **path-change** | **probe-failure** | **test-complete** | **test-failure** }

Default

No traps are sent to the NMS.

Views

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP tracert operation view

ICMP jitter/UDP jitter/voice operation view

Predefined user roles

network-admin

Parameters

path-change: Sends a trap when the UDP tracert operation detects a different path to the destination.

probe-failure *consecutive-probe-failures*: Sends a trap to the NMS if the number of consecutive probe failures in an operation is greater than or equal to *consecutive-probe-failures.* The value range for the *consecutive-probe-failures* argument is 1 to 15. The system counts the number of consecutive probe failures for each operation, so multiple traps might be sent.

test-complete: Sends a trap to indicate that the operation is completed.

test-failure: Sends a trap when an operation fails. For operations other than UDP tracert operation, the system counts the total number of probe failures in an operation. If the number reaches or exceeds the value for the *accumulate-probe-failures* argument, a trap is sent for the operation failure.

accumulate-probe-failures: Specifies the total number of probe failures in an operation. The value range is 1 to 15. This argument is not supported by the UDP tracert operation.

Usage guidelines

The ICMP jitter, UDP jitter, and voice operations support only the **test-complete** keyword.

The following parameters are not available for the UDP tracert operation:

- The **probe-failure** *consecutive-probe-failures* option.
- The *accumulate-probe-failures* argument.

Examples

Configure the system to send a trap if five or more consecutive probe failures occur in an ICMP echo operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] reaction trap probe-failure 5
```

reaction trigger per-probe

Use **reaction trigger per-probe** to configure the probe result sending on a per-probe basis.

Use **undo reaction trigger per-probe** to restore the default.

Syntax

reaction trigger per-probe

undo reaction trigger per-probe

Default

The probe result is sent to the feature that uses the template after three consecutive failed or successful probes.

Views

ICMP/TCP half open template view

Predefined user roles

network-admin

Usage guidelines

The feature enables the NQA client to send the probe result to the feature that uses the NQA template every time a probe is completed.

If you execute this command and the **reaction trigger probe-fail** command multiple times, the most recent configuration takes effect.

If you execute this command and the **reaction trigger probe-pass** command multiple times, the most recent configuration takes effect.

Examples

In ICMP template view, configure the probe result sending on a per-probe basis.

```
<Sysname> system-view
[Sysname] nqa template icmp icmptplt
[Sysname-nqatplt-icmp-icmptplt] reaction trigger per-probe
```

Related commands

reaction trigger probe-fail

reaction trigger probe-pass

reaction trigger probe-fail

Use **reaction trigger probe-fail** to set the number of consecutive probe failures to determine an operation failure.

Use **undo reaction trigger probe-fail** to restore the default.

Syntax

reaction trigger probe-fail *count*

undo reaction trigger probe-fail

Default

The NQA client notifies the feature of the operation failure when the number of consecutive probe failures reaches 3.

Views

Any NQA template view

Predefined user roles

network-admin

Parameters

count: Specifies the number of consecutive probe failures, in the range of 1 to 15.

Usage guidelines

If the number of consecutive probe failures is reached, the NQA client notifies the feature that uses the NQA template of the operation failure.

If you execute this command and the **reaction trigger per-probe** command multiple times, the most recent configuration takes effect.

Examples

In HTTP template view, configure the NQA client to notify the feature of the operation failure when the number of consecutive probe failures reaches 5.

```
<Sysname> system-view
[Sysname] nqa template http httptplt
[Sysname-nqatplt-http-httptplt] reaction trigger probe-fail 5
```

Related commands

reaction trigger per-probe

reaction trigger probe-pass

reaction trigger probe-pass

Use **reaction trigger probe-pass** to set the number of consecutive successful probes to determine a successful operation event.

Use **undo reaction trigger probe-pass** to restore the default.

Syntax

reaction trigger probe-pass *count*

undo reaction trigger probe-pass

Default

The NQA client notifies the feature of the successful operation event if the number of consecutive successful probes reaches 3.

Views

Any NQA template view

Predefined user roles

network-admin

Parameters

count: Specifies the number of consecutive successful probes, in the range of 1 to 15.

Usage guidelines

If number of consecutive successful probes is reached, the NQA client notifies the feature that uses the template of the successful operation event.

If you execute this command and the **reaction trigger per-probe** command multiple times, the most configuration takes effect.

Examples

In HTTP template view, configure the NQA client to notify the feature of the successful operation event if the number of consecutive successful probes reaches 5.

```
<Sysname> system-view
[Sysname] nqa template http httptplt
[Sysname-nqatplt-http-httptplt] reaction trigger probe-pass 5
```

Related commands

reaction trigger per-probe

reaction trigger probe-fail

resolve-target

Use **resolve-target** to specify the domain name to be resolved in the DNS operation.

Use **undo resolve-target** to restore the default.

Syntax

resolve-target *domain-name*

undo resolve-target

Default

The domain name to be resolved in the DNS operation is not specified.

Views

DNS operation view

DNS template view

Predefined user roles

network-admin

Parameters

domain-name: Specifies the domain name to be resolved. It is a dot-separated case-sensitive string of 1 to 255 characters including letters, digits, hyphens (-), and underscores (_) (for example, aabbcc.com). Each part consists of 1 to 63 characters, and consecutive dots (.) are not allowed.

Examples

Specify **domain1** as the domain name to be resolved.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type dns
[Sysname-nqa-admin-test-dns] resolve-target domain1
```

In DNS template view, specify **domain1** as the domain name to be resolved.

```
<Sysname> system-view
[Sysname] nqa template dns dnstplt
[Sysname-nqatplt-dns-dnstplt] resolve-target domain1
```

resolve-type

Use **resolve-type** to configure the domain name resolution type.

Use **undo resolve-type** to restore the default.

Syntax

resolve-type { **A** | **AAAA** }

undo resolve-type

Default

The domain name resolution type is type A.

Views

DNS template view

Predefined user roles

network-admin

Parameters

A: Specifies the type A queries. A type A query resolves a domain name to a mapped IPv4 address.

AAAA: Specifies the type AAAA queries. A type AAAA query resolves a domain name to a mapped IPv6 address.

Examples

In DNS template view, set the domain name resolution type to **A**.

```
<Sysname> system-view
[Sysname] nqa template dns dnstplt
[Sysname-nqatplt-dns-dnstplt] resolve-type A
```

route-option bypass-route

Use **route-option bypass-route** to enable the routing table bypass feature to test the connectivity to the direct destination.

Use **undo route-option bypass-route** to disable the routing table bypass feature.

Syntax

route-option bypass-route

undo route-option bypass-route

Default

The routing table bypass feature is disabled.

Views

ICMP echo/TCP/UDP echo operation view

DLSw/DNS/FTP/HTTP/SNMP operation view

UDP tracert operation view

ICMP jitter/UDP jitter/voice operation view

Predefined user roles

network-admin

Usage guidelines

When the routing table bypass feature is enabled, the following events occur:

- The routing table is not searched. Packets are sent to the destination on a directly connected network.
- The TTL value in the probe packet is set to 1. The TTL set in the **ttl** command does not take effect.

This command does not take effect if the destination address of the NQA operation is an IPv6 address.

Examples

Enable the routing table bypass feature.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] route-option bypass-route
```

source interface (ICMP echo/UDP tracert operation view)

Use **source interface** to specify the IP address of an interface as the source IP address of probe packets.

Use **undo source interface** to restore the default.

Syntax

source interface *interface-type interface-number*

undo source interface

Default

The probe packets take the primary IP address of the outgoing interface as their source IP address.

Views

ICMP echo operation view

UDP tracert operation view

ICMP template view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

The specified interface must be up. If the interface is down, no probe requests can be sent out.

If you execute this command and the **source ip** or **source ipv6** command for an ICMP echo operation or ICMP template multiple times, the most recent configuration takes effect.

If you execute this command and the **source ip** command for a UDP tracert operation multiple times, the most recent configuration takes effect.

Examples

Specify the IP address of the interface VLAN-interface 1 as the source IP address of ICMP echo request packets.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] source interface vlan-interface 1
```

In ICMP template view, specify the IP address of the interface VLAN-interface 1 as the source IP address of ICMP echo request packets.

```
<Sysname> system-view
[Sysname] nqa template icmp icmptplt
[Sysname-nqatplt-icmp-icmptplt] source interface vlan-interface 1
```

Related commands

source ip

source ipv6

source ip

Use **source ip** to configure the source IPv4 address for probe packets.

Use **undo source ip** to restore the default.

Syntax

source ip *ip-address*

undo source ip

Default

The probe packets takes the primary IP address of their output interface as the source IPv4 address.

Views

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/FTP/HTTP/SNMP operation view

UDP tracert operation view

ICMP jitter/path jitter/UDP jitter/voice operation view

Any NQA template view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the source IPv4 address for probe packets.

Usage guidelines

The specified source IP address must be the IPv4 address of a local interface, and the local interface must be up. Otherwise, no probe packets can be sent out.

For an NQA template, if the source and destination addresses have different IP versions, the source address does not take effect.

If you execute the **source interface** and **source ip** commands multiple times for an ICMP echo operation, ICMP template, or UDP tracert operation, the most recent configuration takes effect.

Examples

Specify 10.1.1.1 as the source IPv4 address for ICMP echo requests.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] source ip 10.1.1.1
```

In ICMP template view, specify 10.1.1.1 as the source IPv4 address for ICMP echo requests.

```
<Sysname> system-view
[Sysname] nqa template icmp icmptplt
[Sysname-nqatplt-icmp-icmptplt] source ip 10.1.1.1
```

Related commands

source interface

source ipv6

Use **source ipv6** to configure the source IPv6 address for probe packets.

Use **undo source ipv6** to restore the default.

Syntax

source ipv6 *ipv6-address*

undo source ipv6

Default

The probe packets takes the IPv6 address of their output interface as the source IPv6 address.

Views

ICMP echo operation view

Any NQA template view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the source IPv6 address for probe packets. IPv6 link-local addresses are not supported.

Usage guidelines

The specified source IPv6 address must be the IPv6 address of a local interface. The local interface must be up. Otherwise, no probe packets can be sent out.

For an NQA template, if the source and destination addresses have different IP versions, the source address does not take effect.

If you execute the **source interface** and **source ipv6** commands multiple times for an ICMP echo operation or ICMP template, the most recent configuration takes effect.

Examples

Specify 1::1 as the source IPv6 address for the ICMP echo operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] source ipv6 1::1
```

In ICMP template view, specify 1::1 as the source IPv6 address for ICMP echo requests.

```
<Sysname> system-view
[Sysname] nqa template icmp icmptplt
[Sysname-nqatplt-icmp-icmptplt] source ipv6 1::1
```

Related commands

source interface

source port

Use **source port** to configure the source port number for probe packets.

Use **undo source port** to restore the default.

Syntax

source port *port-number*

undo source port

Default

The source port number is not specified.

Views

UDP echo operation view

SNMP operation view

UDP tracert operation view

UDP jitter/voice operation view

DNS template view

Predefined user roles

network-admin

Parameters

port-number: Specifies the source port number in the range of 1 to 65535.

Examples

Set the source port number to 8000 for probe packets in the UDP echo operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-echo
[Sysname-nqa-admin-test-udp-echo] source port 8000
```

In DNS template view, set the source port number to 8000 for probe packets in the DNS operation.

```
<Sysname> system-view
[Sysname] nqa template dns dnstplt
[Sysname-nqatplt-dns-dnstplt] source port 8000
```

ssl-client-policy

Use **ssl-client-policy** to specify an SSL client policy for an HTTPS or SSL template.

Use **undo ssl-client-policy** to restore the default.

Syntax

ssl-client-policy *policy-name*

undo ssl-client-policy

Default

No SSL client policy is specified for an HTTPS or SSL template.

Views

HTTPS/SSL template view

Predefined user roles

network-admin

Parameters

policy-name: Specifies an SSL client policy by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

In the HTTPS or SSL operation, the NQA client uses the specified SSL client policy to establish an SSL connection to the server.

Examples

Specify SSL client policy **policy** for SSL template **ssltplt**.

```
<Sysname> system-view
[Sysname] nqa template ssl ssltplt
[Sysname-nqatplt-ssl-ssltplt] ssl-client-policy policy
```

statistics hold-time

Use **statistics hold-time** to set the hold time of statistics groups for an NQA operation.

Use **undo statistics hold-time** to restore the default.

Syntax

statistics hold-time *hold-time*

undo statistics hold-time

Default

The hold time of statistics groups for an NQA operation is 120 minutes.

Views

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

ICMP jitter/path jitter/UDP jitter/voice operation view

Predefined user roles

network-admin

Parameters

hold-time: Specifies the hold time in minutes, in the range of 1 to 1440.

Usage guidelines

A statistics group is deleted when its hold time expires.

Examples

Set the hold time to 3 minutes for statistics groups of the ICMP echo operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] statistics hold-time 3
```

statistics interval

Use **statistics interval** to set the statistics collection interval for an NQA operation.

Use **undo statistics interval** to restore the default.

Syntax

statistics interval *interval*

undo statistics interval

Default

The statistics collection interval is 60 minutes.

Views

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

ICMP jitter/path jitter/UDP jitter/voice operation view

Predefined user roles

network-admin

Parameters

interval: Specifies the interval in minutes, in the range of 1 to 35791394.

Usage guidelines

NQA forms statistics within the same collection interval as a statistics group. To display information about the statistics groups, use the **display nqa statistics** command.

Examples

Configure NQA to collect the ICMP echo operation statistics every 2 minutes.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] statistics interval 2
```

statistics max-group

Use **statistics max-group** to set the maximum number of statistics groups that can be saved.

Use **undo statistics max-group** to restore the default.

Syntax

statistics max-group *number*

undo statistics max-group

Default

A maximum of two statistics groups can be saved.

Views

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

ICMP jitter/path jitter/UDP jitter/voice operation view

Predefined user roles

network-admin

Parameters

number: Specifies the maximum number of statistics groups, in the range of 0 to 100. To disable statistics collection, set the value to 0.

Usage guidelines

When the maximum number of statistics groups is reached and a new statistics group is to be saved, the earliest statistics group is deleted.

Examples

Configure NQA to save a maximum of five statistics groups for the ICMP echo operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] statistics max-group 5
```

target-only

Use **target-only** to perform the path jitter operation only on the destination address.

Use **undo target-only** to restore the default.

Syntax

target-only

undo target-only

Default

NQA performs the path jitter operation to the destination hop by hop.

Views

Path jitter operation view

Predefined user roles

network-admin

Examples

Perform the path jitter operation only on the destination address.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type path-jitter
[Sysname-nqa-admin-test-path-jitter] target-only
```

tos

Use **tos** to set the ToS value in the IP header for probe packets.

Use **undo tos** to restore the default.

Syntax

tos *value*

undo tos

Default

The ToS value in the IP header of probe packets is 0.

Views

Any operation view

Any NQA template view

Predefined user roles

network-admin

Parameters

value: Specifies the ToS value in the range of 0 to 255.

Examples

In ICMP echo operation view, set the ToS value to 1 in the IP header for probe packets.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] tos 1
```

In ICMP template view, set the ToS value to 1 in the IP header for probe packets.

```
<Sysname> system-view
[Sysname] nqa template icmp icmptplt
[Sysname-nqatplt-icmp-icmptplt] tos 1
```

ttl

Use **ttl** to set the maximum number of hops that the probe packets can traverse.

Use **undo ttl** to restore the default.

Syntax

ttl *value*

undo ttl

Default

The maximum number of hops is 30 for probe packets of the UDP tracert operation, and is 20 for probe packets of other types of operations.

Views

ICMP echo/TCP/UDP echo operation view

DLSw/DNS/FTP/HTTP/SNMP operation view

UDP tracert operation view

ICMP jitter/UDP jitter/voice operation view

Any NQA template view

Predefined user roles

network-admin

Parameters

value: Specifies the maximum number of hops that the probe packets can traverse, in the range of 1 to 255.

Usage guidelines

The **route-option bypass-route** command sets the TTL to 1 for probe packets. If you configure both the **route-option bypass-route** and **ttl** commands for an operation, the **ttl** command does not take effect.

For a successful UDP tracert operation, make sure the maximum number of hops is not smaller than the value set in the **init-ttl** command.

Examples

Set the maximum number of hops to 16 for probe packets in the ICMP echo operation.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] ttl 16
```

In ICMP template view, set the maximum number of hops to 16 for probe packets.

```
<Sysname> system-view
[Sysname] nqa template icmp icmptplt
[Sysname-nqatplt-icmp-icmptplt] ttl 16
```

type

Use **type** to specify an NQA operation type and enter its view.

Syntax

type { **dhcp** | **dlsw** | **dns** | **ftp** | **http** | **icmp-echo** | **icmp-jitter** | **path-jitter** | **snmp** | **tcp** | **udp-echo** | **udp-jitter** | **udp-tracert** | **voice** }

Default

No operation type is specified.

Views

NQA operation view

Predefined user roles

network-admin

Parameters

dhcp: Specifies the DHCP operation type.

dlsw: Specifies the DLSw operation type.

dns: Specifies the DNS operation type.

ftp: Specifies the FTP operation type.

http: Specifies the HTTP operation type.

icmp-echo: Specifies the ICMP echo operation type.

icmp-jitter: Specifies the ICMP jitter operation type.

path-jitter: Specifies the path jitter operation type.

snmp: Specifies the SNMP operation type.

tcp: Specifies the TCP operation type.

udp-echo: Specifies the UDP echo operation type.

udp-jitter: Specifies the UDP jitter operation type.

udp-tracert: Specifies the UDP tracert operation type.

voice: Specifies the voice operation type.

Usage guidelines

You can specify only one type for an NQA operation. After that, you can configure the operation type-related settings for the NQA operation. To change the type of the NQA operation, remove the NQA operation in system view, and then re-create the NQA operation.

Examples

Specify FTP as the NQA operation type and enter FTP operation view.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp]
```

url

Use **url** to specify the URL of the destination.

Use **undo url** to restore the default.

Syntax

url *url*

undo url

Default

The destination URL is not specified.

Views

FTP/HTTP operation view

FTP/HTTP/HTTPS template view

Predefined user roles

network-admin

Parameters

url: Specifies the URL of the destination server, a case-sensitive string of 1 to 255 characters. The following table describes the URL format and parameters for different operations.

Operation	URL format	Parameter description
HTTP operation	http://*host*/*resource* http://*host*:*port*/*resource*	The *host* parameter represents the host name of the destination server. The host name is a dot-separated case-sensitive string including letters, digits, hyphens (-), and underscores (_). Host names are composed of series of labels, aabbcc.com for example. Each label consists of 1 to 63 characters. Consecutive dots (.) and question marks are not allowed. For description about the filename parameter, see *Fundamentals Configuration Guide*.
HTTPS operation	https://host/resource https://*host*:*port*/*resource*	
FTP operation	ftp://*host/filename* ftp://*host*:*port*/*filename*	

Examples

Configure the URL that the HTTP operation visits as **http://www.company.com/index.htm**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type http
[Sysname-nqa-admin-test-http] url http://www.company.com/index.html
```

In HTTP template view, configure the URL that the HTTP operation visits as **http://www.company.com/index.htm**.

```
<Sysname> system-view
[Sysname] nqa template http httptplt
[Sysname-nqatplt-http-httptplt] url http://www.company.com/index.html
```

username

Use **username** to specify a username.

Use **undo username** to restore the default.

Syntax

username *username*

undo username

Default

No username is configured.

Views

FTP/HTTP operation view

FTP/HTTP/HTTPS/RADIUS template view

Predefined user roles

network-admin

Parameters

username: Specifies the username. This argument is case sensitive. It is a string of 1 to 32 characters for an FTP, HTTP, or HTTPS username, and a string of 1 to 253 characters for a RADIUS authentication username.

Examples

Set the FTP login username to **administrator**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp] username administrator
```

Set the FTP login username to **administrator** in FTP template view.

```
<Sysname> system-view
[Sysname] nqa template ftp ftptplt
[Sysname-nqatplt-ftp-ftptplt] username administrator
```

Related commands

operation

password

version

Use **version** to specify the version used in the HTTP or HTTPS operation.

Use **undo version** to restore the default.

Syntax

version { **v1.0** | **v1.1** }

undo version

Default

Version 1.0 is used in the HTTP operation or HTTPS operation.

Views

HTTP operation view

HTTP/HTTPS template view

Predefined user roles

network-admin

Parameters

v1.0: Uses version 1.0.

v1.1: Uses version 1.1.

Examples

Configure the HTTP operation to use the HTTP version 1.1.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type http
[Sysname-nqa-admin-test-http] version v1.1
```

NQA server commands

IMPORTANT:

Configure the NQA server only for UDP jitter, TCP, UDP echo, and voice operations.

display nqa server

Use **display nqa server status** to display NQA server status.

Syntax

display nqa server

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display NQA server status.

```
<Sysname> display nqa server
NQA server status: Enabled
TCP connect:
   IP address          Port      Tos    VPN instance
   2.2.2.2             2000      200    -
UDP echo:
   IP address          Port      Tos    VPN instance
   3.3.3.3             3000      255    -
```

Table 10 Command output

Field	Description
NQA server status	Whether the NQA server is enabled.
TCP connect	Information about the TCP listening service on the NQA server.
UDP echo	Information about the UDP listening service on the NQA server.

Field	Description
IP address	IP address specified for the TCP/UDP listening service on the NQA server.
Port	Port number specified for the TCP/UDP listening service on the NQA server.
Tos	ToS value in the reply packets sent by the NQA server. The ToS value can be specified when you configure a TCP or UDP listening service on the NQA server. If no ToS value is specified, the following rules apply: • This field displays a hyphen (-). • The ToS value in the reply packets of a TCP listening service is 0. • The ToS value in the reply packets of a UDP listening service is obtained from the request packets.
VPN instance	This field is not supported in the current software version. Name of the VPN instance to which the IP address that the NQA server listens on belongs. This field displays a hyphen (-) if the NQA server listens on a public IP address.

Related commands

`nqa server enable`

`nqa server tcp-connect`

`nqa server udp-echo`

nqa server enable

Use **`nqa server enable`** to enable the NQA server.

Use **`undo nqa server enable`** to disable the NQA server.

Syntax

`nqa server enable`

`undo nqa server enable`

Default

The NQA server is disabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable the NQA server.

```
<Sysname> system-view
[Sysname] nqa server enable
```

Related commands

`display nqa server`

`nqa server tcp-connect`

`nqa server udp-echo`

nqa server tcp-connect

Use **nqa server tcp-connect** to configure a TCP listening service to enable the NQA server to listen to a port on an IP address.

Use **undo nqa server tcp-connect** to remove a TCP listening service.

Syntax

nqa server tcp-connect *ip-address port-number* [**tos** *tos*]

undo nqa server tcp-connect *ip-address port-number*

Default

No TCP listening services exist.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address for the TCP listening service.

port-number: Specifies the port number for the TCP listening service, in the range of 1 to 65535.

tos *tos*: Specifies the ToS value in the IP header for reply packets. The value range is 0 to 255, and the default value is 0.

Usage guidelines

Use this command on the NQA server only for the TCP operation.

When you configure the IP address and port number for a TCP listening service on the NQA server, follow these restrictions and guidelines:

- The IP address and port number must be unique on the NQA server and match the configuration on the NQA client.
- The IP address must be the address of an interface on the NQA server.
- To ensure successful NQA operations and avoid affecting existing services, do not configure the TCP listening service on well-known ports from 1 to 1023.

Examples

Configure a TCP listening service to enable the NQA server to listen to port 9000 on the IP address 169.254.10.2.

```
<Sysname> system-view
[Sysname] nqa server tcp-connect 169.254.10.2 9000
```

Related commands

display nqa server

nqa server enable

nqa server udp-echo

Use **nqa server udp-echo** to configure a UDP listening service to enable the NQA server to listen to a port on an IP address.

Use **undo nqa server udp-echo** to remove the UDP listening service created.

Syntax

nqa server udp-echo *ip-address port-number* [**tos** *tos*]

undo nqa server udp-echo *ip-address port-number*

Default

No UDP listening services exist.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address for the UDP listening service.

port-number: Specifies the port number for the UDP listening service, in the range of 1 to 65535.

tos *tos*: Specifies the ToS value in the IP header for reply packets. The value range is 0 to 255. If you do not specify a ToS value, the ToS value in the request packet is used.

Usage guidelines

Use this command on the NQA server only for the UDP jitter, UDP echo, and voice operations.

When you configure the IP address and port number for a UDP listening service on the NQA server, follow these restrictions and guidelines:

- The IP address and port number must be unique on the NQA server and match the configuration on the NQA client.
- The IP address must be the address of an interface on the NQA server.
- To ensure successful NQA operations and avoid affecting existing services, do not configure the UDP listening service on well-known ports from 1 to 1023.

Examples

Configure a UDP listening service to enable the NQA server to listen to port 9000 on the IP address 169.254.10.2.

```
<Sysname> system-view
[Sysname] nqa server udp-echo 169.254.10.2 9000
```

Related commands

display nqa server

nqa server enable

Contents

NTP commands

NTP is supported only on Layer 3 interfaces.

display ntp-service ipv6 sessions

Use **display ntp-service ipv6 sessions** to display information about all IPv6 NTP associations.

Syntax

display ntp-service ipv6 sessions [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

verbose: Displays detailed information about all IPv6 NTP associations. If you do not specify this keyword, the command displays only brief information about the IPv6 NTP associations.

Examples

Display brief information about all IPv6 NTP associations.

```
<Sysname> display ntp-service ipv6 sessions
Notes: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured.

 Source:   [125]3000::32
 Reference: 127.127.1.0          Clock stratum: 2
 Reachabilities: 1               Poll interval: 64
 Last receive time: 6            Offset: -0.0
 Roundtrip delay: 0.0            Dispersion: 0.0

 Total sessions : 1
```

Table 1 Command output

Field	Description
[12345]	• **1**—Clock source selected by the system (the current reference source). • **2**—The stratum level of the clock source is less than or equal to 15. • **3**—The clock source has survived the clock selection algorithm. • **4**—The clock source is a candidate clock source. • **5**—The clock source was created by a command.
Source	IPv6 address of the NTP server. If this field displays **::**, the IPv6 address of the NTP server has not been resolved successfully.

Field	Description

Reference	Reference clock ID of the NTP server:
	• If the reference clock is the local clock, the value of this field is related to the value of the **Clock stratum** field:
	  ○ When the value of the **Clock stratum** field is 0 or 1, this field displays **LOCL**.
	  ○ When the **Clock stratum** field has another value, this field displays the MD5 digest value of the first 32 bits of the IPv6 address. The MD5 digest value is in dotted decimal format.
	• If the reference clock is the clock of another device on the network, this field displays the MD5 digest value of the first 32 bits of the IPv6 address. The MD5 digest value is in dotted decimal format. If this field displays **INIT**, the local device has not established a connection with the NTP server.

Clock stratum	Stratum level of the NTP server, which determines the clock accuracy. The value is in the range of 1 to 16. A lower stratum level represents higher clock accuracy. A stratum 16 clock is not synchronized.
Reachabilities	Reachability count of the NTP server. 0 indicates that the NTP server is unreachable.
Poll interval	Polling interval in seconds. It is the maximum interval between successive NTP messages.
Last receive time	Length of time from when the last NTP message was received or when the local clock was last updated to the current time. Time is in seconds by default. • If the time length is greater than 2048 seconds, it is displayed in minutes (m). • If the time length is greater than 300 minutes, it is displayed in hours (h). • If the time length is greater than 96 hours, it is displayed in days (d). • If the time length is greater than 999 days, it is displayed in years (y). If the time when the most recent NTP message was received or when the local clock was updated most recently is behind the current time, this field displays a hyphen (-).
Offset	Offset of the system clock relative to the reference clock, in milliseconds.
Roundtrip delay	Roundtrip delay from the local device to the clock source, in milliseconds.
Dispersion	Maximum error of the system clock relative to the reference source.
Total sessions	Total number of associations.

Display detailed information about all IPv6 NTP associations.

```
<Sysname> display ntp-service ipv6 sessions verbose

 Clock source: 1::1
 Session ID: 36144
 Clock stratum: 16
 Clock status:  configured, insane, valid, unsynced
 Reference clock ID: INIT
 Local mode: sym_active, local poll interval: 6
 Peer mode: unspec, peer poll interval: 10
 Offset: 0.0000ms, roundtrip delay: 0.0000ms, dispersion:  15937ms
 Root roundtrip delay: 0.0000ms, root dispersion: 0.0000ms
 Reachabilities:0, sync distance: 15.938
```

```
Precision: 2^-19, version: 4, source interface: Not specified
Reftime: 00000000.00000000  Thu, Feb  7 2036  6:28:16.000
Orgtime: d17cbb21.0f318106  Tue, May 17 2011  9:15:13.059
Rcvtime: 00000000.00000000  Thu, Feb  7 2036  6:28:16.000
Xmttime: 00000000.00000000  Thu, Feb  7 2036  6:28:16.000
Roundtrip delay samples: 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000
Offset samples: 0.00  0.00  0.00  0.00  0.00  0.00  0.00  0.00
Filter order: 0     1     2     3     4     5     6     7

Total sessions: 1
```

Table 2 Command output

Field	Description
Clock source	IPv6 address of the clock source. If this field displays **::**, the IPv6 address of the NTP server has not been resolved successfully.
Clock stratum	Stratum level of the NTP server, which determines the clock precision. The value is in the range of 1 to 16. A lower stratum level represents higher clock accuracy. A stratum 16 clock is not synchronized.

Clock status	Status of the clock source corresponding to this association:
	• **configured**—The association was created at the CLI.
	• **dynamic**—The association is established dynamically.
	• **master**—The clock source is the primary NTP server of the current system.
	• **selected**—The clock source has survived the clock selection algorithm.
	• **candidate**—The clock source is the candidate reference source.
	• **sane**—The clock source has passed authentication and its clock will be used as the reference clock.
	• **insane**—The clock source has not passed authentication, or it has passed authentication but its clock will not be used as the reference clock.
	• **valid**—The clock source is valid, which means the clock source meets the following requirements:
	  ○ It has been authenticated and synchronized.
	  ○ Its stratum level is valid.
	  ○ Its root delay and root dispersion values are within their ranges.
	• **invalid**—The clock source is invalid.
	• **unsynced**—The clock source has not been synchronized or the value of the stratum level is invalid.

Reference clock ID	• If the reference clock is the local clock, the value of this field is related to the value of the Clock stratum field:
	  ○ When the value of the Clock stratum field is 0 or 1, this field displays **LOCL**.
	  ○ When the Clock stratum field has another value, this field displays the MD5 digest value of the first 32 bits of the IPv6 address. The MD5 digest value is in dotted decimal format.
	• If the reference clock is the clock of another device on the network, this field displays the MD5 digest value of the first 32 bits of the IPv6 address. The MD5 digest value is in dotted decimal format. If this field displays **INIT**, the local device has not established a connection with the NTP server.

Field	Description
Local mode	Operation mode of the local device: • **unspec**—The mode is unspecified. • **sym_active**—Active mode. • **sym_passive**—Passive mode. • **client**—Client mode. • **server**—Server mode. • **broadcast**—Broadcast or multicast server mode. • **bclient**—Broadcast or multicast client mode.
local poll interval	Polling interval for the local device, in seconds. The value displayed is a power of 2. For example, if the displayed value is 6, the poll interval of the local device is 2^6, or 64 seconds.
peer mode	Operation mode of the peer device: • **unspec**—The mode is unspecified. • **sym_active**—Active mode. • **sym_passive**—Passive mode. • **client**—Client mode. • **server**—Server mode. • **broadcast**—Broadcast or multicast server mode. • **bclient**—Broadcast or multicast client mode.
peer poll interval	Polling interval for the peer device, in seconds. The value displayed is a power of 2. For example, if the displayed value is 6, the polling interval of the local device is 2^6, or 64 seconds.
Offset	Offset of the system clock relative to the reference clock, in milliseconds.
roundtrip delay	Roundtrip delay from the local device to the clock source, in milliseconds.
dispersion	Maximum error of the system clock relative to the reference clock.
Root roundtrip delay	Roundtrip delay from the local device to the primary NTP server, in milliseconds.
root dispersion	Maximum error of the system clock relative to the primary NTP server, in milliseconds.
Reachabilities	Reachability count of the clock source. 0 indicates that the clock source is unreachable.
sync distance	Synchronization distance relative to the upper-level clock, in seconds, and calculated from dispersion and roundtrip delay values.
Precision	Accuracy of the system clock.
version	NTP version in the range of 1 to 4.
source interface	Source interface. If the source interface is not specified, this field displays **Not specified**.
Reftime	Reference timestamp in the NTP message.
Orgtime	Originate timestamp in the NTP message.
Rcvtime	Receive timestamp in the NTP message.
Xmttime	Transmit timestamp in the NTP message.
Filter order	Dispersion information.

Field	Description
Reference clock status	Status of the local clock. The field is displayed only when you use the **ntp-service refclock-master** command to set the local clock as the reference clock. When the reach field of the local clock is 255, the field is displayed as **working normally**. Otherwise, the field is displayed as **working abnormally**.
Total sessions	Total number of associations.

display ntp-service sessions

Use **display ntp-service sessions** to display information about all IPv4 NTP associations.

Syntax

display ntp-service sessions [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

verbose: Displays detailed information about all IPv4 NTP associations. If you do not specify this keyword, the command displays only brief information about the NTP associations.

Usage guidelines

When a device is operating in NTP broadcast or multicast server mode, the **display ntp-service sessions** command does not display the IPv4 NTP association information corresponding to the broadcast or multicast server. However, the associations are counted in the total number of associations.

Examples

Display brief information about all IPv4 NTP associations.

```
<Sysname> display ntp-service sessions
       source          reference       stra reach poll  now offset  delay disper
**********************************************************************************
[12345]LOCAL(0)        LOCL               0     1   64    - 0.0000 0.0000 7937.9
    [5]0.0.0.0         INIT              16     0   64    - 0.0000 0.0000 0.0000
Notes: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured.
 Total sessions: 1
```

Table 3 Command output

Field	Description
source	• When the reference clock is the local clock, the field displays **LOCAL** (*number*). It indicates that the IP address of the local clock is 127.127.1.*number*, where *number* represents the NTP process number in the range of 0 to 3. • When the reference clock is the clock of another device, the field displays the IP address of the NTP server. If this field displays **0.0.0.0**, the IP address of the NTP server has not been resolved successfully.

Field	Description

reference	Reference clock ID of the NTP server:
	• If the reference clock is the local clock, the value of this field is related to the value of the **stra** field:
	  ○ When the value of the **stra** field is 0 or 1, this field displays **LOCL**.
	  ○ When the **stra** field has another value, this field displays the IP address of the local clock.
	• If the reference clock is the clock of another device on the network, this field displays the IP address of the device. If the device supports IPv6, this field displays the MD5 digest of the first 32 bits of the IPv6 address of the device. If this field displays **INIT**, the local device has not established a connection with the NTP server.

stra	Stratum level of the clock source, which determines the clock accuracy. The value is in the range of 1 to 16. The clock accuracy decreases from stratum 1 to stratum 16. A stratum 1 clock has the highest precision, and a stratum 16 clock is not synchronized.
reach	Reachability count of the clock source. 0 indicates that the clock source is unreachable.
poll	Polling interval in seconds. It is the maximum interval between successive NTP messages.
now	Length of time from when the last NTP message was received or when the local clock was last updated to the current time. Time is in seconds by default. • If the time length is greater than 2048 seconds, it is displayed in minutes (m). • If the time length is greater than 300 minutes, it is displayed in hours (h). • If the time length is greater than 96 hours, it is displayed in days (d). • If the time length is greater than 999 days, it is displayed in years (y). If the time when the most recent NTP message was received or when the local clock was updated most recently is behind the current time, this field displays a hyphen (-).
offset	Offset of the system clock relative to the reference clock, in milliseconds.
delay	Roundtrip delay from the local device to the NTP server, in milliseconds.
disper	Maximum error of the system clock relative to the reference source, in milliseconds.
[12345]	• **1**—Clock source selected by the system (the current reference source). • **2**—The stratum level of the clock source is less than or equal to 15. • **3**—The clock source has survived the clock selection algorithm. • **4**—The clock source is a candidate clock source. • **5**—The clock source was created by a configuration command.
Total sessions	Total number of associations.

Display detailed information about all IPv4 NTP associations.

```
<Sysname> display ntp-service sessions verbose
 Clock source: 192.168.1.40
 Session ID: 35888
 Clock stratum: 2
 Clock status:  configured, master, sane, valid
 Reference clock ID: 127.127.1.0
 Local mode: client, local poll interval: 6
 Peer mode: server, peer poll interval: 6
 Offset: 0.2862ms, roundtrip delay: 3.2653ms, dispersion: 4.5166ms
```

```
Root roundtrip delay: 0.0000ms, root dispersion: 10.910ms
Reachabilities:31, sync distance: 0.0194
Precision: 2^-19, version: 3, source interface: Not specified
Reftime: d17cbba5.1473de1e  Tue, May 17 2011  9:17:25.079
Orgtime: 00000000.00000000  Thu, Feb  7 2036  6:28:16.000
Rcvtime: d17cbbc0.b1959a30  Tue, May 17 2011  9:17:52.693
Xmttime: d17cbbc0.b1959a30  Tue, May 17 2011  9:17:52.693
Roundtrip delay samples: 0.007 0.010 0.006 0.011 0.010 0.005 0.007 0.003
Offset samples: 5629.55 3913.76 5247.27 6526.92 31.99 148.72 38.27 0.29
Filter order: 7     5     2     6     0     4     1     3

Total sessions: 1
```

Table 4 Command output

Field	Description
Clock source	IP address of the NTP server. If this field displays **0.0.0.0**, the IP address of the NTP server has not been resolved successfully.
Clock stratum	Stratum level of the NTP server, which determines the clock accuracy. The value is in the range of 1 to 16. A lower stratum level represents greater clock accuracy. A stratum 16 clock is not synchronized.

Clock status	Status of the clock source corresponding to this association:
	• **configured**—The association was created by a configuration command.
	• **dynamic**—The association is established dynamically.
	• **master**—The clock source is the primary NTP server of the current system.
	• **selected**—The clock source has survived the clock selection algorithm.
	• **candidate**—The clock source is the candidate reference source.
	• **sane**—The clock source has passed authentication and its clock will be used as the reference clock.
	• **insane**—The clock source has not passed authentication, or it has passed authentication but its clock will not be used as the reference clock.
	• **valid**—The clock source is valid, which means the clock source meets the following requirements:
	  ○ It has been authenticated and synchronized.
	  ○ Its stratum level is valid.
	  ○ Its root delay and root dispersion values are within their ranges.
	• **invalid**—The clock source is invalid.
	• **unsynced**—The clock source has not been synchronized or the value of the stratum level is invalid.

Reference clock ID	Reference clock ID of the NTP server:
	• If the reference clock is the local clock, the value of this field is related to the value of the **Clock** stratum field:
	  ○ When the value of the **Clock** stratum field is 0 or 1, this field displays **LOCL**.
	  ○ When the **Clock** stratum field has another value, this field displays the IP address of the local clock.
	• If the reference clock is the clock of another device on the network, this field displays the IP address of the device. If the device supports IPv6, this field displays the MD5 digest of the first 32 bits of the IPv6 address of the device. If this field displays **INIT**, the local device has not established a connection with the NTP server.

Field	Description
Local mode	Operation mode of the local device: • **unspec**—The mode is unspecified. • **active**—Active mode. • **passive**—Passive mode. • **client**—Client mode. • **server**—Server mode. • **broadcast**—Broadcast or multicast server mode. • **bclient**—Broadcast or multicast client mode.
local poll interval	Polling interval of the local device, in seconds. The value displayed is a power of 2. For example, if the displayed value is 6, the poll interval of the local device is 2^6, or 64 seconds.
Peer mode	Operation mode of the peer device: • **unspec**—The mode is unspecified. • **active**—Active mode. • **passive**—Passive mode. • **client**—Client mode. • **server**—Server mode. • **broadcast**—Broadcast or multicast server mode. • **bclient**—Broadcast or multicast client mode.
peer poll interval	Polling interval of the peer device, in seconds. The value displayed is a power of 2. For example, if the displayed value is 6, the poll interval of the local device is 2^6, or 64 seconds.
Offset	Offset of the system clock relative to the reference clock, in milliseconds.
roundtrip delay	Roundtrip delay from the local device to the NTP server, in milliseconds.
dispersion	Maximum error of the system clock relative to the reference clock.
Root roundtrip delay	Roundtrip delay from the local device to the primary NTP server, in milliseconds.
root dispersion	Maximum error of the system clock relative to the primary reference clock, in milliseconds.
Reachabilities	Reachability count of the clock source. 0 indicates that the clock source is unreachable.
sync distance	Synchronization distance relative to the upper-level clock, in seconds, and calculated from dispersion and roundtrip delay values.
Precision	Accuracy of the system clock.
version	NTP version in the range of 1 to 4.
source interface	Source interface. If the source interface is not specified, this field is **Not specified**.
Reftime	Reference timestamp in the NTP message.
Orgtime	Originate timestamp in the NTP message.
Rcvtime	Receive timestamp in the NTP message.
Xmttime	Transmit timestamp in the NTP message.
Filter order	Sample information order.

Field	Description
Reference clock status	Status of the local clock. The field is displayed only when you use the **ntp-service refclock-master** command to set the local clock as the reference clock. When the reach field of the local clock is 255, the field is displayed as **working normally**. Otherwise, the field is displayed as **working abnormally**.
Total sessions	Total number of associations.

display ntp-service status

Use **display ntp-service status** to display NTP service status.

Syntax

display ntp-service status

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display NTP service status after time synchronization.

```
<Sysname> display ntp-service status
 Clock status: synchronized
 Clock stratum: 2
 System peer: LOCAL(0)
 Local mode: client
 Reference clock ID: 127.127.1.0
 Leap indicator: 00
 Clock jitter: 0.000977 s
 Stability: 0.000 pps
 Clock precision: 2^-19
 Root delay: 0.00000 ms
 Root dispersion: 3.96367 ms
 Reference time: d0c5fc32.92c70b1e  Wed, Dec 29 2010 18:28:02.573
 System poll interval: 256 s
```

Display the NTP service status when time is not synchronized.

```
<Sysname> display ntp-service status
 Clock status: unsynchronized
 Clock stratum: 16
 Reference clock ID: none
 Clock jitter: 0.000000 s
 Stability: 0.000 pps
 Clock precision: 2^-19
 Clock precision:
 Root delay: 0.00000 ms
 Root dispersion: 0.00002 ms
```

```
Reference time: d0c5fc32.92c70b1e  Wed, Dec 29 2010 18:28:02.573
System poll interval: 8 s
```

Table 5 Command output

Field	Description
Clock status	Status of the system clock: • **synchronized**—The system clock has been synchronized. • **unsynchronized**—The system clock has not been synchronized.
Clock stratum	Stratum level of the system clock.
System peer	IP address of the selected NTP server.
Local mode	Operation mode of the local device: • **unspec**—The mode is unspecified. • **active**—Active mode. • **passive**—Passive mode. • **client**—Client mode. • **server**—Server mode. • **broadcast**—Broadcast or multicast server mode. • **bclient**—Broadcast or multicast client mode.
Reference clock ID	For an IPv4 NTP server: The field represents the IP address of the remote server when the local device is synchronized to a remote NTP server. The field represents the local clock when the local device uses the local clock as the reference source. • When the local clock has a stratum level of 1, this field displays **LOCL**. • When the local clock has any other stratum, this field displays the IP address of the local clock. For an IPv6 NTP server: The field represents the MD5 digest of the first 32 bits of the IPv6 address of the remote server when the local device is synchronized to a remote IPv6 NTP server. The field represents the local clock when the local device uses the local clock as the reference source. • When the local clock has a stratum level of 1, this field displays **LOCL**. • When the local clock has any other stratum, this field displays the MD5 digest of the first 32 bits of the IPv6 address of the local clock.
Leap indicator	Alarming status: • **00**—Normal. • **01**—Leap second, indicates that the last minute in a day has 61 seconds. • **10**—Leap second, indicates that the last minute in a day has 59 seconds. • **11**—Time is not synchronized.
Clock jitter	Difference between the system clock and reference clock, in seconds.
Stability	Clock frequency stability. A lower value represents better stability.
Clock precision	Accuracy of the system clock.
Root delay	Roundtrip delay from the local device to the primary NTP server, in milliseconds.
Root dispersion	Maximum error of the system clock relative to the primary NTP server, in milliseconds.
Reference time	Reference timestamp.
System poll interval	System polling interval in seconds.

display ntp-service trace

Use **display ntp-service trace** to display brief information about each NTP server from the local device back to the primary NTP server.

Syntax

display ntp-service trace [**source** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

source *interface-type interface-number*: Specifies the source interface for sending NTP packets to trace each NTP server from the local device back to the primary NTP server. The source IP address of the NTP packets is the IPv4 address/IPv6 address of the specified source interface. If the IP address of an NTP server is a link-local address, the link-local address of the outgoing interface of NTP packets is used as the source IP address of the NTP packets. If you do not specify this option, the interface that sends the tracing NTP packets acts as the source interface.

Usage guidelines

To trace back to the primary NTP server from the source interface, make sure the source interface and the NTP servers from the local device to the primary NTP server are reachable to each other.

Examples

Display brief information about each NTP server from the local device back to the primary NTP server.

```
<Sysname> display ntp-service trace
Server     127.0.0.1
Stratum    3, jitter  0.000, synch distance 0.0000.
Server     3000::32
Stratum    2 , jitter 790.00, synch distance 0.0000.
RefID      127.127.1.0
```

The output shows that server 127.0.0.1 is synchronized to server 3000::32, and server 3000::32 is synchronized to the local clock.

Table 6 Command output

Field	Description
Server	IP address of the NTP server.
Stratum	Stratum level of the NTP server.
jitter	Root mean square (RMS) value of the clock offset relative to the upper-level clock, in seconds.
synch distance	Synchronization distance relative to the upper-level NTP server, in seconds, calculated from dispersion and roundtrip delay values.
RefID	Identifier of the primary NTP server. When the stratum level of the primary reference clock is 0, it is displayed as **LOCL**. Otherwise, it is displayed as the IP address of the primary reference clock.

Related commands

ntp-service ipv6 source

ntp-service ipv6 unicast-server

ntp-service ipv6 unicast-peer

ntp-service source

ntp-service unicast-server

ntp-service unicast-peer

ntp-service acl

Use **ntp-service acl** to configure the right for peer devices to access the IPv4 NTP services on the local device.

Use **undo ntp-service** to remove the configured IPv4 NTP service access right.

Syntax

ntp-service { **peer** | **query** | **server** | **synchronization** } **acl** *ipv4-acl-number*

undo ntp-service { **peer** | **query** | **server** | **synchronization** } [**acl** *ipv4-acl-number*]

Default

The right for the peer devices to access the IPv4 NTP services on the local device is **peer**.

Views

System view

Predefined user roles

network-admin

Parameters

peer: Allows time requests and NTP control queries (such as alarms, authentication status, and time server information) from a peer device and allows the local device to synchronize itself to a peer device.

query: Allows only NTP control queries from a peer device to the local device.

server: Allows time requests and NTP control queries from a peer device, but does not allow the local device to synchronize itself to a peer device.

synchronization: Allows only time requests from a peer device.

acl *ipv4-acl-number*: Specifies an IPv4 ACL by its number. The peer devices that match the IPv4 ACL have the access right specified in the command. The *ipv4-acl-number* argument represents an IPv4 basic ACL number in the range of 2000 to 2999 or an IPv4 advanced ACL number in the range of 3000 to 3999.

Usage guidelines

When the device receives an IPv4 NTP request, it matches the request against the access rights in order from the least restrictive to the most restrictive: **peer**, **server**, **synchronization**, and **query**.

- If no IPv4 NTP access control is configured, the **peer** access right applies.
- If the IP address of the peer device matches a **permit** statement in an IPv4 ACL, the access right is granted to the peer device. If a **deny** statement or no IPv4 ACL is matched, no access right is granted.

- If no IPv4 ACL is specified for an access right or the IPv4 ACL specified for the access right is not created, the access right is not granted.
- If none of the IPv4 ACLs specified for the access rights is created, the **peer** access right applies.
- If none of the IPv4 ACLs specified for the access rights contains rules, no access right is granted.

The **ntp-service acl** command provides minimal security for a system running NTP. A more secure method is NTP authentication.

Examples

Configure the peer devices on subnet 10.10.0.0/16 to have full access to the local device.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] ntp-service peer acl 2001
```

Related commands

ntp-service authentication enable

ntp-service authentication-keyid

ntp-service reliable authentication-keyid

ntp-service authentication enable

Use **ntp-service authentication enable** to enable NTP authentication.

Use **undo ntp-service authentication enable** to disable NTP authentication.

Syntax

ntp-service authentication enable

undo ntp-service authentication enable

Default

NTP authentication is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Enable NTP authentication in networks that require time synchronization security to make sure NTP clients are synchronized only to authenticated NTP servers.

To authenticate an NTP server, set an authentication key and specify it as a trusted key.

Examples

Enable NTP authentication.

```
<Sysname> system-view
[Sysname] ntp-service authentication enable
```

Related commands

ntp-service authentication-keyid

ntp-service reliable authentication-keyid

ntp-service authentication-keyid

Use **ntp-service authentication-keyid** to set an NTP authentication key.

Use **undo ntp-service authentication-keyid** to remove an NTP authentication key.

Syntax

ntp-service authentication-keyid *keyid* **authentication-mode** { **hmac-sha-1** | **hmac-sha-256** | **hmac-sha-384** | **hmac-sha-512** | **md5** } { **cipher** | **simple** } *string* [**acl** *ipv4-acl-number* | **ipv6 acl** *ipv6-acl-number*] *

undo ntp-service authentication-keyid *keyid*

Default

No NTP authentication key exists.

Views

System view

Predefined user roles

network-admin

Parameters

keyid: Specifies an authentication key ID in the range of 1 to 4294967295.

authentication-mode: Specifies an authentication algorithm.

- **hmac-sha-1**: Specifies the HMAC-SHA-1 algorithm.
- **hmac-sha-256**: Specifies the HMAC-SHA-256 algorithm.
- **hmac-sha-384**: Specifies the HMAC-SHA-384 algorithm.
- **hmac-sha-512**: Specifies the HMAC-SHA-512 algorithm.
- **md5**: Specifies the MD5 algorithm.

cipher: Specifies an authentication key in encrypted form.

simple: Specifies an authentication key in plaintext form. For security purposes, the authentication key specified in plaintext form will be stored in encrypted form.

string: Specifies a case-sensitive authentication key. Its plaintext form is a string of 1 to 32 characters. Its encrypted form is a string of 1 to 73 characters.

acl *ipv4-acl-number*: Specifies an IPv4 basic ACL by its number in the range of 2000 to 2999. Only the devices permitted by the ACL can use the key ID for authentication.

ipv6 acl *ipv6-acl-number*: Specifies an IPv6 basic ACL by its number in the range of 2000 to 2999. Only the devices permitted by the ACL can use the key ID for authentication.

Usage guidelines

In a network where there is a high security demand, the NTP authentication feature must be enabled for a system running NTP. This feature enhances the network security by using client-server key authentication, which prohibits a client from synchronizing to a device that has failed the authentication.

The key ID in the message from the peer device identifies the key used for authentication. The **acl** *ipv4-acl-number* or **acl** *ipv6-acl-number* option is used to identify the peer device that can use the key ID.

- The device uses the **acl** *ipv4-acl-number* or **acl** *ipv6-acl-number* option to identify the peer device that can use the key ID only when an NTP session for the peer device is required to be established or after the NTP session has been established.
- If the specified IPv4 or IPv6 ACL does not exist, any device can use the key ID for authentication.
- If the specified IPv4 or IPv6 ACL does not contain any rules, no device can use the key ID for authentication.

To ensure a successful NTP authentication, configure the same key ID, authentication algorithm, and key on the time server and client.

After you specify an NTP authentication key, use the **ntp-service reliable authentication-keyid** command to configure the key as a trusted key. The key automatically changes to untrusted after you delete the key. In this case, you do not need to execute the **undo ntp-service reliable authentication-keyid** command.

The security strength of the five algorithms, in descending order, is HMAC-SHA-512, HMAC-SHA-384, HMAC-SHA-256, HMAC-SHA-1, and MD5.

You can set a maximum of 128 authentication keys by executing the command.

Examples

Set a plaintext MD5 authentication key, with the key ID of **10** and key value of **BetterKey**.

```
<Sysname> system-view
[Sysname] ntp-service authentication enable
[Sysname] ntp-service authentication-keyid 10 authentication-mode md5 simple BetterKey
```

Related commands

ntp-service authentication enable

ntp-service reliable authentication-keyid

ntp-service broadcast-client

Use **ntp-service broadcast-client** to configure the device to operate in NTP broadcast client mode and use the current interface to receive NTP broadcast packets.

Use **undo ntp-service broadcast-client** to remove the configuration.

Syntax

ntp-service broadcast-client

undo ntp-service broadcast-client

Default

The device does not operate in any NTP association mode.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

After you configure the command, the device listens to NTP messages sent by the NTP broadcast server and is synchronized based on the received NTP messages.

If you have configured the device to operate in broadcast client mode on an interface with the command, do not add the interface to any aggregate group. To add the interface to an aggregate group, remove the configuration of the command.

Examples

Configure the device to operate in broadcast client mode and receive NTP broadcast messages on VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service broadcast-client
```

Related commands

ntp-service broadcast-server

ntp-service broadcast-server

Use **ntp-service broadcast-server** to configure the device to operate in NTP broadcast server mode and use the current interface to send NTP broadcast packets.

Use **undo ntp-service broadcast-server** to remove the configuration.

Syntax

ntp-service broadcast-server [**authentication-keyid** *keyid* | **version** *number*] *

undo ntp-service broadcast-server

Default

The device does not operate in any NTP association mode.

Views

Interface view

Predefined user roles

network-admin

Parameters

authentication-keyid *keyid*: Specifies the key ID to be used for sending broadcast messages to broadcast clients. The value range for the *keyid* argument is 1 to 4294967295. If you do not specify this option, the local device cannot synchronize broadcast clients enabled with NTP authentication.

version *number*: Specifies the NTP version. The value range for the *number* argument is 1 to 4, and the default is 4.

Usage guidelines

After you configure the command, the device periodically sends NTP messages to the broadcast address 255.255.255.255.

If you have configured the device to operate in broadcast server mode on an interface with the command, do not add the interface to any aggregate group. To add the interface to an aggregate group, remove the configuration of the command.

Examples

Configure the device to operate in broadcast server mode and send NTP broadcast messages on VLAN-interface 1, using key 4 for encryption. Set the NTP version to 4.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service broadcast-server authentication-keyid 4 version 4
```

Related commands

ntp-service broadcast-client

ntp-service dscp

Use **ntp-service dscp** to set a DSCP value for IPv4 NTP packets.

Use **undo ntp-service dscp** to restore the default.

Syntax

ntp-service dscp *dscp-value*

undo ntp-service dscp

Default

The DSCP value for IPv4 NTP packets is 48.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Sets a DSCP value in the range of 0 to 63 for IPv4 NTP packets.

Usage guidelines

The DSCP value is included in the ToS field of an IPv4 packet to identify the packet priority.

Examples

Set the DSCP value for IPv4 NTP packets to **30**.

```
<Sysname> system-view
[Sysname] ntp-service dscp 30
```

ntp-service enable

Use **ntp-service enable** to enable the NTP service.

Use **undo ntp-service enable** to disable the NTP service.

Syntax

ntp-service enable

undo ntp-service enable

Default

The NTP service is disabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable the NTP service.

```
<Sysname> system-view
[Sysname] ntp-service enable
```

ntp-service inbound enable

Use **ntp-service inbound enable** to enable an interface to receive NTP messages.

Use **undo ntp-service inbound enable** to disable an interface from receiving NTP messages.

Syntax

ntp-service inbound enable

undo ntp-service inbound enable

Default

An interface receives NTP messages.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

Execute the **undo ntp-service inbound enable** command on an interface in the following cases:

- You do not want the interface to synchronize the peer device in the corresponding subnet.
- You do not want the device to be synchronized by the peer device in the subnet corresponding to the interface.

Examples

Disable VLAN-interface 1 from receiving NTP messages.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] undo ntp-service inbound enable
```

ntp-service ipv6 acl

Use **ntp-service ipv6 acl** to configure the right for the peer devices to access the IPv6 NTP services of the local device.

Use **undo ntp-service ipv6** to remove the configured IPv6 NTP service access right.

Syntax

ntp-service ipv6 { **peer** | **query** | **server** | **synchronization** } **acl** *ipv6-acl-number*

undo ntp-service ipv6 { **peer** | **query** | **server** | **synchronization** } [**acl** *ipv6-acl-number*]

Default

The right for the peer devices to access the IPv6 NTP services on the local device is **peer**.

Views

System view

Predefined user roes

network-admin

Parameters

peer: Allows time requests and NTP control queries (such as alarms, authentication status, and time server information) and allows the local device to synchronize itself to a peer device.

query: Allows only NTP control queries from a peer device to the local device.

server: Allows time requests and NTP control queries, but does not allow the local device to synchronize itself to a peer device.

synchronization: Allows only time requests from a system whose address passes the access list criteria.

ipv6-acl-number: Specifies an IPv6 ACL by its number. The peer devices that match the IPv6 ACL have the access right specified in the command. The *ipv6-acl-number argument* represents a basic IPv6 ACL number in the range of 2000 to 2999 or an advanced IPv6 ACL number in the range of 3000 to 3999.

Usage guidelines

When the device receives an IPv6 NTP request, it matches the request against the access rights in order from the least restrictive to the most restrictive: **peer**, **server**, **synchronization**, and **query**.

- If no IPv6 NTP access control is configured, the **peer** access right applies.
- If the IP address of the peer device matches a **permit** statement in an IPv6 ACL, the access right is granted to the peer device. If a **deny** statement or no IPv6 ACL is matched, no access right is granted.
- If no IPv6 ACL is specified for an access right or the IPv6 ACL specified for the access right is not created, the access right is not granted.
- If none of the IPv6 ACLs specified for the access rights is created, the **peer** access right applies.
- If none of the IPv6 ACLs specified for the access rights contains rules, no access right is granted.

The **ntp-service ipv6 acl** command provides a minimum security method. NTP authentication is more secure.

Examples

Configure the peer devices on subnet 2001::1 to have full access to the local device.

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2001
[Sysname-acl-ipv6-basic-2001] rule permit source 2001::1 64
[Sysname-acl-ipv6-basic-2001] quit
[Sysname] ntp-service ipv6 peer acl 2001
```

Related commands

ntp-service authentication enable

ntp-service authentication-keyid

ntp-service reliable authentication-keyid

ntp-service ipv6 dscp

Use **ntp-service ipv6 dscp** to set a DSCP value for IPv6 NTP packets.

Use **undo ntp-service ipv6 dscp** to restore the default.

Syntax

ntp-service ipv6 dscp *dscp-value*

undo ntp-service ipv6 dscp

Default

The DSCP value for IPv6 NTP packets is 56.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63 for IPv6 NTP packets.

Usage guidelines

The DSCP value is included in the Traffic Class field of an IPv6 packet to identify the packet priority.

Examples

Set the DSCP value for IPv6 NTP packets to **30**.

```
<Sysname> system-view
[Sysname] ntp-service ipv6 dscp 30
```

ntp-service ipv6 inbound enable

Use **ntp-service ipv6 inbound enable** to enable an interface to receive IPv6 NTP messages.

Use **undo ntp-service ipv6 inbound enable** to disable an interface from receiving IPv6 NTP messages.

Syntax

ntp-service ipv6 inbound enable

undo ntp-service ipv6 inbound enable

Default

An interface receives IPv6 NTP messages.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

Execute the **undo ntp-service ipv6 inbound enable** command on an interface in the following cases:

- You do not want the interface to synchronize the peer devices in the corresponding subnet.
- You do not want the device to be synchronized by the peer devices in the subnet corresponding to the interface.

Examples

Disable VLAN-interface 1 from receiving IPv6 NTP messages.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] undo ntp-service ipv6 inbound enable
```

ntp-service ipv6 multicast-client

Use **ntp-service ipv6 multicast-client** to configure the device to operate in IPv6 NTP multicast client mode and use the current interface to receive IPv6 NTP multicast packets.

Use **undo ntp-service ipv6 multicast-client** to remove the configuration.

Syntax

ntp-service ipv6 multicast-client *ipv6-address*

undo ntp-service ipv6 multicast-client *ipv6-address*

Default

The device does not operate in any NTP association mode.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies an IPv6 multicast address. An IPv6 broadcast client and an IPv6 broadcast server must be configured with the same multicast address.

Usage guidelines

After you configure the command, the device listens to IPv6 NTP messages using the specified multicast address as the destination address. It is synchronized based on the received IPv6 NTP messages.

If you have configured the device to operate in IPv6 multicast client mode on an interface by using the command, do not add the interface to any aggregate group. To add the interface to an aggregate group, remove the configuration of the command.

Examples

Configure the device to operate in IPv6 multicast client mode and receive IPv6 NTP multicast messages with the destination FF21::1 on VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service ipv6 multicast-client ff21::1
```

Related commands

ntp-service ipv6 multicast-server

ntp-service ipv6 multicast-server

Use **ntp-service ipv6 multicast-server** to configure the device to operate in IPv6 NTP multicast server mode and use the current interface to send IPv6 NTP multicast packets.

Use **undo ntp-service ipv6 multicast-server** to remove the configuration.

Syntax

ntp-service ipv6 multicast-server *ipv6-address* [**authentication-keyid** *keyid* | **ttl** *ttl-number*] *

undo ntp-service ipv6 multicast-server *ipv6-address*

Default

The device does not operate in any NTP association mode.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies an IPv6 multicast address. An IPv6 multicast client and server must be configured with the same multicast address.

authentication-keyid *keyid*: Specifies the key ID to be used for sending multicast messages to multicast clients. The value range for the *keyid* argument is 1 to 4294967295. If you do not specify this option, the local device cannot synchronize clients enabled with NTP authentication.

ttl *ttl-number*: Specifies the TTL of NTP multicast messages. The value range for the *ttl-number* argument is 1 to 255, and the default is 16.

Usage guidelines

After you configure the command, the device periodically sends NTP messages to the specified IPv6 multicast address.

If you have configured the device to operate in IPv6 multicast server mode on an interface with the command, do not add the interface to any aggregate group. To add the interface to an aggregate group, remove the configuration of the command.

Examples

Configure the device to operate in IPv6 multicast server mode and send IPv6 NTP multicast messages on VLAN-interface 1 to the multicast address FF21::1, using key 4 for encryption.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service ipv6 multicast-server ff21::1 authentication-keyid
4
```

Related commands

ntp-service ipv6 multicast-client

ntp-service ipv6 source

Use **ntp-service ipv6 source** to specify a source interface for IPv6 NTP messages.

Use **undo ntp-service ipv6 source** to restore the default.

Syntax

ntp-service ipv6 source *interface-type interface-number*

undo ntp-service ipv6 source

Default

No source interface is specified for IPv6 NTP messages. The device automatically selects the source IP address for IPv6 NTP messages. For more information, see *RFC 3484*.

Views

System view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

If you specify a source interface for IPv6 NTP messages, the device uses the IPv6 address of the source interface as the source address to send IPv6 NTP messages. Consequently, the destination address of the IPv6 NTP response messages is the address of the source interface.

When the device responds to an IPv6 NTP request, the source IPv6 address of the NTP response is always the IPv6 address of the interface that has received the IPv6 NTP request.

If you do not want the IPv6 address of an interface on the local device to become the destination address for response messages, use the command to specify another interface as the source interface for IPv6 NTP messages.

The source interface for IPv6 NTP messages can also be specified in the following ways:

- In NTP client/server mode, if you have specified the source interface for IPv6 NTP messages in the **ntp-service ipv6 unicast-server** command, the specified interface acts as the source interface for IPv6 NTP messages.
- In NTP symmetric active/passive mode, if you have specified the source interface for IPv6 NTP messages in the **ntp-service ipv6 unicast-peer** command, the specified interface acts as the source interface for IPv6 NTP messages.
- In NTP multicast mode, if you have configured the **ntp-service ipv6 multicast-server** command on an interface, the interface acts as the source interface for NTP multicast messages.

If the specified source interface is down, the device does not send IPv6 NTP messages.

Examples

Specify the source interface of IPv6 NTP messages as VLAN-interface 1.

```
<Sysname> system-view
[Sysname] ntp-service ipv6 source vlan-interface 1
```

ntp-service ipv6 unicast-peer

Use **ntp-service ipv6 unicast-peer** to specify an IPv6 symmetric-passive peer for the device.

Use **undo ntp-service ipv6 unicast-peer** to remove the IPv6 symmetric-passive peer specified for the device.

Syntax

ntp-service ipv6 unicast-peer { *peer-name* | *ipv6-address* } [**authentication-keyid** *keyid* | **maxpoll** *maxpoll-interval* | **minpoll** *minpoll-interval* | **priority** | **source** *interface-type interface-number*] *

undo ntp-service ipv6 unicast-peer { *peer-name* | *ipv6-address* }

Default

No IPv6 symmetric-passive peer is specified.

Views

System view

Predefined user roles

network-admin

Parameters

peer-name: Specifies a symmetric-passive peer by its host name, a case-insensitive string of 1 to 253 characters.

ipv6-address: Specifies a symmetric-passive peer by its IPv6 address. It must be a unicast address, rather than a multicast address.

authentication-keyid *keyid*: Specifies the key ID to be used for sending NTP messages to the peer. The value range for the *keyid* argument is 1 to 4294967295. If you do not specify this option, the local device and the peer do not authenticate each other.

maxpoll *maxpoll-interval*: Specifies the maximum polling interval. The value range for the *maxpoll-interval* argument is 4 to 17, to which base 2 is raised to get the interval in seconds. The maximum polling interval is in the range of 2^4 to 2^{17} (16 to 131072) seconds. The default value for the *maxpoll-interval* argument is 6 and the default maximum polling interval is 2^6 (64) seconds.

minpoll *minpoll-interval*: Specifies the minimum polling interval. The value range for the *minpoll-interval* argument is 4 to 17, to which base 2 is raised to get the interval in seconds. The minimum polling interval is in the range of 2^4 to 2^{17} (16 to 131072) seconds. The default value for the *minpoll-interval* argument is 6 and the default minimum polling interval is 2^6 (64) seconds.

priority: Specifies the peer specified by *ipv6-address* or *peer-name* as the first choice under the same condition.

source *interface-type interface-number*: Specifies the source interface for IPv6 NTP messages. If the specified passive peer address is not a link local address, the source IPv6 address for IPv6 NTP messages sent by the local device is the IPv6 address of the specified source interface. If the specified passive peer address is a link local address, the IPv6 NTP messages are sent from the specified source interface, and the source address of the messages is the link local address of the interface. The *interface-type interface-number* argument represents the interface type and number. If you do not specify an interface, the device automatically selects the source IPv6 address of IPv6 NTP messages. For more information, see *RFC 3484*.

Usage guidelines

When you specify an IPv6 passive peer for the device, the device and its IPv6 passive peer can be synchronized to each other. If their clocks are in synchronized state, the clock with a high stratum level is synchronized to the clock with a lower stratum level.

If the specified IPv6 address of the passive peer is a link local address, you must specify the source interface for NTP messages.

After you specify an IPv6 symmetric-passive peer for a device, the device polls and synchronize its time with the peer device at the minimum polling interval. If the time discrepancy between the two remains in the acceptable range, the system gradually increases the polling interval until the

maximum polling interval is reached. If the time discrepancy exceeds the acceptable range repeatedly, the polling interval decreases gradually.

The polling interval configuration takes effect when the next polling starts.

Examples

Specify the device with the IPv6 address of 2001::1 as the symmetric-passive peer of the device, and specify the source interface for IPv6 NTP messages as VLAN-interface 1.

```
<Sysname> system-view
[Sysname] ntp-service ipv6 unicast-peer 2001::1 source vlan-interface 1
```

Related commands

ntp-service authentication enable

ntp-service authentication-keyid

ntp-service reliable authentication-keyid

ntp-service ipv6 unicast-server

Use **ntp-service ipv6 unicast-server** to specify an IPv6 NTP server for the device.

Use **undo ntp-service ipv6 unicast-server** to remove an IPv6 NTP server specified for the device.

Syntax

ntp-service ipv6 unicast-server { *server-name* | *ipv6-address* } [**authentication-keyid** *keyid* | **maxpoll** *maxpoll-interval* | **minpoll** *minpoll-interval* | **priority** | **source** *interface-type interface-number*] *

undo ntp-service ipv6 unicast-server { *server-name* | *ipv6-address* }

Default

No IPv6 NTP server is specified.

Views

System view

Predefined user roles

network-admin

Parameters

server-name: Specifies an NTP server by its host name, a case-insensitive string of 1 to 253 characters.

ipv6-address: Specifies an NTP server by its IPv6 address. It must be a unicast address, rather than a multicast address.

authentication-keyid *keyid*: Specifies the key ID to be used for sending NTP messages to the NTP server. The value range for the *keyid* argument is 1 to 4294967295. If you do not specify this option, the local device and NTP server do not authenticate each other.

maxpoll *maxpoll-interval*: Specifies the maximum polling interval. The value range for the *maxpoll-interval* argument is 4 to 17, to which base 2 is raised to get the interval in seconds. The maximum polling interval is in the range of 2^4 to 2^{17} (16 to 131072) seconds. The default value for the *maxpoll-interval* argument is 6 and the default maximum polling interval is 2^6 (64) seconds.

minpoll *minpoll-interval*: Specifies the minimum polling interval. The value range for the *minpoll-interval* argument is 4 to 17, to which base 2 is raised to get the interval in seconds.

The minimum polling interval is in the range of 2^4 to 2^{17} (16 to 131072) seconds. The default value for the *minpoll-interval* argument is 6 and the default minimum polling interval is 2^6 (64) seconds.

priority: Specifies this NTP server as the first choice under the same condition.

source *interface-type interface-number*: Specifies the source interface for IPv6 NTP messages. If the specified IPv6 NTP server address is not a link local address, the source IPv6 address for IPv6 NTP messages sent by the local device to the NTP server is the IPv6 address of the specified source interface. If the specified IPv6 NTP server address is a link local address, the IPv6 NTP messages are sent from the specified source interface, and the source address of the messages is the link local address of the interface. The *interface-type interface-number* argument represents the interface type and number. If you do not specify an interface, the device automatically selects the source IPv6 address of IPv6 NTP messages. For more information, see *RFC 3484*.

Usage guidelines

When you specify an IPv6 NTP server for the device, the device is synchronized to the IPv6 NTP server, but the IPv6 NTP server is not synchronized to the device.

If the specified IPv6 address of the NTP server is a link local address, you must specify the source interface for NTP messages.

After you specify an IPv6 NTP server for a device, the device polls and synchronizes its time with the server at the minimum polling interval. If the time discrepancy between the two remains in the acceptable range, the system gradually increases the polling interval until the maximum polling interval is reached. If the time discrepancy exceeds the acceptable range repeatedly, the polling interval decreases gradually.

The polling interval configuration takes effect when the next polling starts.

Examples

Specify the IPv6 NTP server 2001::1 for the device.

```
<Sysname> system-view
[Sysname] ntp-service ipv6 unicast-server 2001::1
```

Related commands

ntp-service authentication enable

ntp-service authentication-keyid

ntp-service reliable authentication-keyid

ntp-service max-dynamic-sessions

Use **ntp-service max-dynamic-sessions** to set the maximum number of dynamic NTP sessions.

Use **undo ntp-service max-dynamic-sessions** to restore the default.

Syntax

ntp-service max-dynamic-sessions *number*

undo ntp-service max-dynamic-sessions

Default

The maximum number of dynamic NTP sessions is 100.

Views

System view

Predefined user roles

network-admin

Parameters

number: Sets the maximum number of dynamic NTP associations, in the range of 0 to 100.

Usage guidelines

A device can have a maximum of 128 concurrent associations, including static associations and dynamic associations. A static association refers to an association that a user has manually created by using an NTP command. A dynamic association is a temporary association created by the system during operation.

This command limits the number of dynamic NTP associations and prevents dynamic NTP associations from occupying too many system resources.

Examples

Set the maximum number of dynamic NTP associations to 50.

```
<Sysname> system-view
[Sysname] ntp-service max-dynamic-sessions 50
```

Related commands

display ntp-service sessions

ntp-service multicast-client

Use **ntp-service multicast-client** to configure the device to operate in NTP multicast client mode and use the current interface to receive NTP multicast packets.

Use **undo ntp-service multicast-client** to remove the NTP multicast client configuration.

Syntax

ntp-service multicast-client [*ip-address*]

undo ntp-service multicast-client [*ip-address*]

Default

The device does not operate in any NTP association mode.

Views

Interface view

Predefined user roles

network-admin

Parameters

ip-address: Specifies a multicast IP address. The default value is 224.0.1.1. The value for the *ip-address* argument is 224.0.1.0/24.The multicast client and multicast server must be configured with the same multicast IP address.

Usage guidelines

After you configure the command, the device listens to NTP messages using the specified multicast address as the destination address.

If you have configured the device to operate in multicast client mode on an interface with the command, do not add the interface to any aggregate group. To add the interface to an aggregate group, remove the NTP multicast client configuration from the interface.

Examples

Configure the device to operate in multicast client mode and receive NTP multicast messages on VLAN-interface 1, and set the multicast address to 224.0.1.1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service multicast-client 224.0.1.1
```

Related commands

ntp-service multicast-server

ntp-service multicast-server

Use **ntp-service multicast-server** to configure the device to operate in NTP multicast server mode and use the current interface to send NTP multicast packets.

Use **undo ntp-service multicast-server** to remove the NTP multicast server configuration.

Syntax

ntp-service multicast-server [*ip-address*] [**authentication-keyid** *keyid* | **ttl** *ttl-number* | **version** *number*] *

undo ntp-service multicast-server [*ip-address*]

Default

The device does not operate in any NTP association mode.

Views

Interface view

Predefined user roles

network-admin

Parameters

ip-address: Specifies a multicast IP address. The default value is 224.0.1.1. The value for the *ip-address* argument is 224.0.1.0/24.The multicast server and client must be configured with the same multicast IP address.

authentication-keyid *keyid*: Specifies the key ID to be used for sending multicast messages to multicast clients. The value range for the *keyid* argument is 1 to 4294967295. If you do not specify this option, the local device cannot synchronize multicast clients enabled with NTP authentication.

ttl *ttl-number*: Specifies the TTL of NTP multicast messages. The value range for the *ttl-number* argument is 1 to 255. The default value is 16.

version *number*: Specifies the NTP version. The value range for the *number* argument is 1 to 4. The default value is 4.

Usage guidelines

After you configure the command, the device periodically sends NTP messages to the specified multicast address.

If you have configured the device to operate in multicast server mode on an interface with the command, do not add the interface to any aggregate group. To add the interface to an aggregate group, remove the NTP multicast server configuration from the interface.

Examples

Configure the device to operate in multicast server mode and send NTP multicast messages on VLAN-interface 1 to the multicast address 224.0.1.1, using key 4 for encryption. Set the NTP version to 4.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service multicast-server 224.0.1.1 version 4
authentication-keyid 4
```

Related commands

ntp-service multicast-client

ntp-service refclock-master

Use **ntp-service refclock-master** to configure the local clock as the reference source.

Use **undo ntp-service refclock-master** to remove the configuration.

Syntax

ntp-service refclock-master [*ip-address*] [*stratum*]

undo ntp-service refclock-master [*ip-address*]

Default

The device does not use its local clock as the reference clock.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: IP address of the local clock, 127.127.1.*u*, where *u* is the NTP process ID in the range of 0 to 3. The default value is 127.127.1.0.

stratum: Stratum level of the local clock, in the range of 1 to 15. The default value is 8. A lower stratum level represents higher clock accuracy.

Usage guidelines

Typically an NTP server that gets its time from an authoritative time source, such as an atomic clock has stratum 1 and operates as the primary time server to provide time synchronization for other devices in the network. The accuracy of each server is the stratum, with the topmost level (primary servers) assigned as one and each level downwards (secondary servers) in the hierarchy assigned as one greater than the preceding level.

If the devices in a network cannot synchronize to an authoritative time source, you can perform the following tasks:

- Select a device that has a relatively accurate clock from the network.
- Use the local clock of the device as the reference clock to synchronize other devices in the network.

Use the command with caution to avoid time errors. As a best practice, set the local clock time to a correct value before you execute the command.

Examples

Specify the local clock as the reference source, with the stratum level 2.

```
<Sysname> system-view
[Sysname] ntp-service refclock-master 2
```

ntp-service reliable authentication-keyid

Use **ntp-service reliable authentication-keyid** to specify an authentication key as a trusted key.

Use **undo ntp-service reliable authentication-keyid** to remove the configuration.

Syntax

ntp-service reliable authentication-keyid *keyid*

undo ntp-service reliable authentication-keyid *keyid*

Default

No trusted key is specified.

Views

System view

Predefined user roles

network-admin

Parameters

keyid: Specifies an authentication key by its ID in the range of 1 to 4294967295.

Usage guidelines

When NTP authentication is enabled, a client can be synchronized only to a server that can provide a trusted authentication key.

Before you use the command, make sure NTP authentication is enabled and an authentication key is configured. The key automatically changes to untrusted after you delete the key. In this case, you do not need to execute the **undo ntp-service reliable authentication-keyid** command.

You can set a maximum of 128 keys by executing the command.

Examples

Enable NTP authentication, specify the MD5 algorithm, with the key ID of 37 and key value of **BetterKey**.

```
<Sysname> system-view
[Sysname] ntp-service authentication enable
[Sysname] ntp-service authentication-keyid 37 authentication-mode md5 simple BetterKey
```

Specify this key as a trusted key.

```
[Sysname] ntp-service reliable authentication-keyid 37
```

Related commands

ntp-service authentication enable

ntp-service authentication-keyid

ntp-service source

Use **ntp-service source** to specify a source IPv4 address for NTP messages.

Use **undo ntp-service source** to restore the default.

Syntax

ntp-service source { *interface-type interface-number* | *ipv4-address* }

undo ntp-service source

Default

No source IPv4 address is specified for NTP messages. The device performs the following operations:

- Searches the routing table for the outbound interface of NTP messages.
- Uses the primary IPv4 address of the outbound interface as the source IPv4 address for NTP messages.

Views

System view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you specify a source interface for NTP messages, the device uses the primary IPv4 address of the specified source interface as the source address to send NTP messages. The receiving device uses this address as the destination address of the NTP response message.

ip-address: Specifies the source IPv4 address for NTP messages.

Usage guidelines

When the device responds to an NTP request, the source IP address of the NTP response is always the IP address of the interface that has received the NTP request.

If you have specified the source interface for NTP messages in the **ntp-service unicast-server** or **ntp-service unicast-peer** command, the IPv4 address of the specified interface is used as the source IPv4 address for NTP messages.

If you have configured the **ntp-service broadcast-server** or **ntp-service multicast-server** command in an interface view, the IPv4 address of the interface is used as the source IPv4 address for broadcast or multicast NTP messages.

If the specified source interface is down, the device does not send NTP messages.

Examples

Specify the IP address of VLAN-interface 1 as the source IPv4 address for NTP messages.

```
<Sysname> system-view
[Sysname] ntp-service source vlan-interface 1
```

ntp-service time-offset-threshold

Use **ntp-service time-offset-threshold** to set the NTP time-offset thresholds for log and trap outputs.

Use **undo ntp-service time-offset-threshold** to restore the default.

Syntax

ntp-service time-offset-threshold { **log** *log-threshold* | **trap** *trap-threshold* } *

undo ntp-service time-offset-threshold

Default

No NTP time-offset thresholds are set for log and trap outputs.

Views

System view

Predefined user roles

network-admin

Parameters

log *log-threshold*: Specifies the NTP time-offset threshold for log output. The value range for the *log-threshold* argument is 128 to 60000, in milliseconds.

trap *trap-threshold*: Specifies the NTP time-offset threshold for trap output. The value range for the *trap-threshold* argument is 128 to 60000, in milliseconds.

Usage guidelines

By default, the system synchronizes the NTP client's time to the server and outputs a log and a trap when the time offset exceeds 128 ms for multiple times.

After you set the thresholds, the system synchronizes the client's time to the server when the time offset exceeds 128 ms for multiple times, but outputs logs and traps only when the time offset exceeds the specified thresholds, respectively.

Examples

Set the NTP time-offset thresholds for log and trap outputs to 500 ms and 600 ms, respectively.

```
<Sysname> system-view
[Sysname] ntp-service time-offset-threshold log 500 trap 600
```

ntp-service unicast-peer

Use **ntp-service unicast-peer** to specify a symmetric-passive peer for the device.

Use **undo ntp-service unicast-peer** to remove the symmetric-passive peer specified for the device.

Syntax

ntp-service unicast-peer { *peer-name* | *ip-address* } [**authentication-keyid** *keyid* | **maxpoll** *maxpoll-interval* | **minpoll** *minpoll-interval* | **priority** | **source** *interface-type interface-number* | **version** *number*] *

undo ntp-service unicast-peer { *peer-name* | *ip-address* }

Default

No symmetric-passive peer is specified.

Views

System view

Predefined user roles

network-admin

Parameters

peer-name: Specifies a symmetric-passive peer by its host name, a case-insensitive string of 1 to 253 characters.

ip-address: Specifies a symmetric-passive peer by its IP address. It must be a unicast address, rather than a broadcast address, a multicast address, or the IP address of the local clock.

authentication-keyid *keyid*: Specifies the key ID to be used for sending NTP messages to the peer. The value range for the *keyid* argument is 1 to 4294967295. If you do not specify this option, the local device and the peer do not authenticate each other.

maxpoll *maxpoll-interval*: Specifies the maximum polling interval. The value range for the *maxpoll-interval* argument is 4 to 17, to which base 2 is raised to get the interval in seconds. The maximum polling interval is in the range of 2^4 to 2^{17} (16 to 131072) seconds. The default value for the *maxpoll-interval* argument is 6 and the default maximum polling interval is 2^6 (64) seconds.

minpoll *minpoll-interval*: Specifies the minimum polling interval. The value range for the *minpoll-interval* argument is 4 to 17, to which base 2 is raised to get the interval in seconds. The minimum polling interval is in the range of 2^4 to 2^{17} (16 to 131072) seconds. The default value for the *minpoll-interval* argument is 6 and the default minimum polling interval is 2^6 (64) seconds.

priority: Specifies the peer specified by *ip-address* or *peer-name* as the first choice under the same condition.

source *interface-type interface-number*: Specifies the source interface for NTP messages. In an NTP message the local device sends to its peer, the source IP address is the primary IP address of this interface. The *interface-type interface-number* argument represents the interface type and number. If you do not specify this option, the device searches the routing table for the outgoing interface and uses the primary IP address of the outgoing interface as the source IP address of the NTP messages.

version *number*: Specifies the NTP version. The value range for the *number* argument is 1 to 4. The default value is 4.

Usage guidelines

When you specify a passive peer for the device, the device and its passive peer can be synchronized to each other. If their clocks are in synchronized state, the clock with a high stratum level is synchronized to the clock with a lower stratum level.

Examples

Specify the device with the IP address of 10.1.1.1 as the symmetric-passive peer of the device, and configure the device to run NTP version 4. Specify the source interface of NTP messages as VLAN-interface 1.

```
<Sysname> system-view
[Sysname] ntp-service unicast-peer 10.1.1.1 version 4 source-interface vlan-interface 1
```

Related commands

ntp-service authentication enable

ntp-service authentication-keyid

ntp-service reliable authentication-keyid

ntp-service unicast-server

Use **ntp-service unicast-server** to specify an NTP server for the device.

Use **undo ntp-service unicast-server** to remove an NTP server specified for the device.

Syntax

ntp-service unicast-server { *server-name* | *ip-address* } [**authentication-keyid** *keyid* | **maxpoll** *maxpoll-interval* | **minpoll** *minpoll-interval* | **priority** | **source** *interface-type interface-number* | **version** *number*] *

undo ntp-service unicast-server { *server-name* | *ip-address* }

Default

No NTP server is specified.

Views

System view

Predefined user roles

network-admin

Parameters

server-name: Specifies an NTP server by its host name, a case-insensitive string of 1 to 253 characters.

ip-address: Specifies an NTP server by its IP address. It must be a unicast address, rather than a broadcast address, a multicast address, or the IP address of the local clock.

authentication-keyid *keyid*: Specifies the key ID to be used for sending NTP messages to the NTP server. The value range for the *keyid* argument is 1 to 4294967295. If you do not specify this option, the local device and NTP server do not authenticate each other.

maxpoll *maxpoll-interval*: Specifies the maximum polling interval. The value range for the *maxpoll-interval* argument is 4 to 17, to which base 2 is raised to get the interval in seconds. The maximum polling interval is in the range of 2^4 to 2^{17} (16 to 131072) seconds. The default value for the *maxpoll-interval* argument is 6 and the default maximum polling interval is 2^6 (64) seconds.

minpoll *minpoll-interval*: Specifies the minimum polling interval. The value range for the *minpoll-interval* argument is 4 to 17, to which base 2 is raised to get the interval in seconds. The minimum polling interval is in the range of 2^4 to 2^{17} (16 to 131072) seconds. The default value for the *minpoll-interval* argument is 6 and the default minimum polling interval is 2^6 (64) seconds.

priority: Specifies this NTP server as the first choice under the same condition.

source *interface-type interface-number*: Specifies the source interface for NTP messages. For an NTP message the local device sends to the NTP server, the source IP address is the primary IP address of this interface. The *interface-type interface-number* argument represents the interface type and number. If you do not specify this option, the device searches the routing table for the outgoing interface and uses the primary IP address of the outgoing interface as the source IP address of the NTP messages.

version *number*: Specifies the NTP version. The value range for the *number* argument is 1 to 4. The default value is 4.

Usage guidelines

When you specify an NTP server for the device, the device is synchronized to the NTP server, but the NTP server is not synchronized to the device.

Examples

Specify NTP server 10.1.1.1 for the device, and configure the device to run NTP version 4.

```
<Sysname> system-view
[Sysname] ntp-service unicast-server 10.1.1.1 version 4
```

Related commands

ntp-service authentication enable

ntp-service authentication-keyid

ntp-service reliable authentication-keyid

SNTP commands

display sntp ipv6 sessions

Use **display sntp ipv6 sessions** to display information about all IPv6 SNTP associations.

Syntax

display sntp ipv6 sessions

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display information about all IPv6 SNTP associations.

```
<Sysname> display sntp ipv6 sessions
SNTP server: 2001::1
Stratum: 16
Version: 4
Last receive time: No packet was received.

SNTP server: 2001::100
Stratum: 3
Version: 4
Last receive time: Fri, Oct 21 2011 11:28:28.058 (Synced)
```

Table 7 Command output

Field	Description
SNTP server	SNTP server (NTP server). If this field displays **::**, the IPv6 address of the NTP server has not been resolved successfully.
Stratum	Stratum level of the NTP server, which determines the clock accuracy. It is in the range of 1 to 16. A lower stratum level represents a higher clock accuracy. A clock with stratum level 16 is not synchronized.
Version	SNTP version.
Last receive time	Time when the last message was received: • **Synced**—The local clock is synchronized to the NTP server. • **No packet was received**—The device has not received any SNTP session information from the server.

display sntp sessions

Use **display sntp sessions** to display information about all IPv4 SNTP associations.

Syntax

display sntp sessions

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display information about all IPv4 SNTP associations.

```
<Sysname> display sntp sessions
SNTP server     Stratum   Version    Last receive time
1.0.1.11        2         4          Tue, May 17 2011  9:11:20.833 (Synced)
```

Table 8 Command output

Field	Description
SNTP server	SNTP server (NTP server). If this field displays **0.0.0.0**, the IP address of the NTP server has not been resolved successfully.
Stratum	Stratum level of the NTP server, which determines the clock accuracy. It is in the range of 1 to 16. A lower stratum level represents higher clock accuracy. A clock with stratum level 16 is not synchronized.
Version	SNTP version.
Last receive time	Time when the last message was received. Synced means the local clock is synchronized to the NTP server.

sntp authentication enable

Use **sntp authentication enable** to enable SNTP authentication.

Use **undo sntp authentication enable** to disable SNTP authentication.

Syntax

sntp authentication enable

undo sntp authentication enable

Default

SNTP authentication is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

You need to enable SNTP authentication in networks that require time synchronization security to make sure SNTP clients are synchronized only to authenticated NTP servers.

To authenticate an NTP server, set an authentication key and specify it as a trusted key.

Examples

Enable SNTP authentication.

```
<Sysname> system-view
```

```
[Sysname] sntp authentication enable
```

Related commands

sntp authentication-keyid

sntp reliable authentication-keyid

sntp authentication-keyid

Use **sntp authentication-keyid** to set an SNTP authentication key.

Use **undo sntp authentication-keyid** to remove an SNTP authentication key.

Syntax

sntp authentication-keyid *keyid* **authentication-mode** { **hmac-sha-1** | **hmac-sha-256** | **hmac-sha-384** | **hmac-sha-512** | **md5** } { **cipher** | **simple** } *string* [**acl** *ipv4-acl-number* | **ipv6 acl** *ipv6-acl-number*] *

undo sntp authentication-keyid *keyid*

Default

No SNTP authentication key exists.

Views

System view

Predefined user roles

network-admin

Parameters

keyid: Specifies an authentication key ID in the range of 1 to 4294967295.

authentication-mode: Specifies an authentication algorithm.

- **hmac-sha-1**: Specifies the HMAC-SHA-1 algorithm.
- **hmac-sha-256**: Specifies the HMAC-SHA-256 algorithm.
- **hmac-sha-384**: Specifies the HMAC-SHA-384 algorithm.
- **hmac-sha-512**: Specifies the HMAC-SHA-512 algorithm.
- **md5**: Specifies the MD5 algorithm.

cipher: Specifies an authentication key in encrypted form.

simple: Specifies an authentication key in plaintext form. For security purposes, the authentication key specified in plaintext form will be stored in encrypted form.

string: Specifies a case-sensitive authentication key. Its plaintext form is a string of 1 to 32 characters. Its encrypted form is a string of 1 to 73 characters.

acl *ipv4-acl-number*: Specifies an IPv4 basic ACL by its number in the range of 2000 to 2999. Only the devices permitted by the ACL can use the key ID for authentication.

ipv6 acl *ipv6-acl-number*: Specifies an IPv6 basic ACL by its number in the range of 2000 to 2999. Only the devices permitted by the ACL can use the key ID for authentication.

Usage guidelines

You need to enable SNTP authentication in networks that require time synchronization security to make sure SNTP clients are synchronized only to authenticated NTP servers.

The key ID in the message from the peer device identifies the key used for authentication. The **acl** *ipv4-acl-number* or **acl** *ipv6-acl-number* option is used to identify the peer device that can use the key ID.

- The device uses the **acl** *ipv4-acl-number* or **acl** *ipv6-acl-number* option to identify the peer device that can use the key ID only when an SNTP session for the peer device is required to be established or after the SNTP session has been established.
- If the specified IPv4 or IPv6 ACL does not exist, any device can use the key ID for authentication.
- If the specified IPv4 or IPv6 ACL does not contain any rules, no device can use the key ID for authentication.

To ensure a successful authentication, configure the same key ID, authentication algorithm, and key on the time server and client.

After you configure an SNTP authentication key, use the **sntp reliable authentication-keyid** command to set it as a trusted key. The key automatically changes to untrusted after you delete the key. In this case, you do not need to execute the **undo sntp-service reliable authentication-keyid** command.

The security strength of the five algorithms, in descending order, is HMAC-SHA-512, HMAC-SHA-384, HMAC-SHA-256, HMAC-SHA-1, and MD5.

You can set a maximum of 128 authentication keys by executing the command.

Examples

Set an MD5 authentication key, with the key ID of **10** and key value of **BetterKey**. Input the key in plain text.

```
<Sysname> system-view
[Sysname] sntp authentication enable
[Sysname] sntp authentication-keyid 10 authentication-mode md5 simple BetterKey
```

Related commands

sntp authentication enable

sntp reliable authentication-keyid

sntp enable

Use **sntp enable** to enable the SNTP service.

Use **undo sntp enable** to disable the SNTP service.

Syntax

sntp enable

undo sntp enable

Default

The SNTP service is disabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable the SNTP service.

```
<Sysname> system-view
[Sysname] sntp enable
```

sntp ipv6 unicast-server

Use **sntp ipv6 unicast-server** to specify an IPv6 NTP server for the device.

Use **undo sntp ipv6 unicast-server** to remove the IPv6 NTP server specified for the device.

Syntax

sntp ipv6 unicast-server { *server-name* | *ipv6-address* } [**authentication-keyid** *keyid* | **source** *interface-type interface-number*] *

undo sntp ipv6 unicast-server { *server-name* | *ipv6-address* }

Default

No IPv6 NTP server is specified.

Views

System view

Predefined user roles

network-admin

Parameters

server-name: Specifies an NTP server by its host name, a case-insensitive string of 1 to 253 characters.

ipv6-address: Specifies an NTP server by its IPv6 address.

authentication-keyid *keyid*: Specifies the key ID to be used for sending NTP messages to the NTP server. The value range for the *keyid* argument is 1 to 4294967295. If you do not specify this option, the local device and NTP server do not authenticate each other.

source *interface-type interface-number*: Specifies the source interface for IPv6 NTP messages. If the specified IPv6 NTP server address is not a link local address, the source IPv6 address for IPv6 NTP messages sent by the local device to the NTP server is the IPv6 address of the specified source interface. If the specified IPv6 NTP server address is a link local address, the IPv6 NTP messages are sent from the specified source interface, and the source address of the messages is the link local address of the interface. The *interface-type interface-number* argument represents the interface type and number. If you do not specify an interface, the device automatically selects the source IPv6 address of IPv6 NTP messages. For more information, see *RFC 3484*.

Usage guidelines

When you specify an IPv6 NTP server for the device, the device is synchronized to the NTP server, but the NTP server is not synchronized to the device.

Examples

Specify the IPv6 NTP server 2001::1 for the device.

```
<Sysname> system-view
[Sysname] sntp ipv6 unicast-server 2001::1
```

Related commands

sntp authentication enable

sntp authentication-keyid

sntp reliable authentication-keyid

sntp reliable authentication-keyid

Use **sntp reliable authentication-keyid** to specify a trusted key.

Use **undo sntp reliable authentication-keyid** to remove the trusted key.

Syntax

sntp reliable authentication-keyid *keyid*

undo sntp reliable authentication-keyid *keyid*

Default

No trusted key is specified.

Views

System view

Predefined user roles

network-admin

Parameters

keyid: Specifies an authentication key by its ID in the range of 1 to 4294967295.

Usage guidelines

If SNTP is enabled, the SNTP client is synchronized only to an NTP server that provides a trusted key.

Before you use the command, make sure SNTP authentication is enabled and an authentication key is configured. The key automatically changes to untrusted after you delete the key. In this case, you do not need to execute the **undo sntp-service reliable authentication-keyid** command.

Examples

Enable NTP authentication, and specify the MD5 encryption algorithm, with the key ID of 37 and key value of **BetterKey**.

```
<Sysname> system-view
[Sysname] sntp authentication enable
[Sysname] sntp authentication-keyid 37 authentication-mode md5 simple BetterKey
```

Specify this key as a trusted key.

```
[Sysname] sntp reliable authentication-keyid 37
```

Related commands

sntp authentication-keyid

sntp authentication enable

sntp time-offset-threshold

Use **sntp time-offset-threshold** to specify the SNTP time-offset thresholds for log and trap outputs.

Use **undo sntp time-offset-threshold** to restore the default.

Syntax

sntp time-offset-threshold { **log** *log-threshold* | **trap** *trap-threshold* } *

undo sntp time-offset-threshold

Default

No SNTP time-offset thresholds are set for log and trap outputs.

Views

System view

Predefined user roles

network-admin

Parameters

log *log-threshold*: Specifies the SNTP time-offset threshold for log output. The value range for the *log-threshold* argument is 128 to 60000, in milliseconds.

trap *trap-threshold*: Specifies the SNTP time-offset threshold for trap output. The value range for the *trap-threshold* argument is 128 to 60000, in milliseconds.

Usage guidelines

By default, the system synchronizes the NTP client's time to the server and outputs a log and a trap when the time offset exceeds 128 ms for multiple times.

After you set the NTP time-offset thresholds for log and trap outputs, the system synchronizes the client's time to the server when the time offset exceeds 128 ms for multiple times, but outputs logs and traps only when the time offset exceeds the specified thresholds, respectively.

Examples

Specify the SNTP time-offset thresholds for log and trap outputs as 500 ms and 600 ms, respectively.

```
<Sysname> system-view
[Sysname] sntp time-offset-threshold log 500 trap 600
```

sntp unicast-server

Use **sntp unicast-server** to specify an NTP server for the device.

Use **undo sntp unicast-server** to remove an NTP server specified for the device.

Syntax

sntp unicast-server { *server-name* | *ip-address* } [**authentication-keyid** *keyid* | **source** *interface-type interface-number* | **version** *number*] *

undo sntp unicast-server { *server-name* | *ip-address* }

Default

No NTP server is specified.

Views

System view

Predefined user roles

network-admin

Parameters

server-name: Specifies an NTP server by its host name, a case-insensitive string of 1 to 253 characters.

ip-address: Specifies an NTP server by its IP address. It must be a unicast address, rather than a broadcast address, a multicast address, or the IP address of the local clock.

authentication-keyid *keyid*: Specifies the key ID to be used for sending NTP messages to the NTP server. The value range for the *keyid* argument is 1 to 4294967295. If you do not specify this option, the local device and NTP server do not authenticate each other.

source *interface-type interface-number*: Specifies the source interface for NTP messages. In an NTP message the local device sends to the NTP server, the source IP address is the primary IP address of this interface. The *interface-type interface-number* argument represents the interface type and number.

version *number*: Specifies the NTP version. The value range for the *number* argument is 1 to 4. The default value is 4.

Usage guidelines

When you specify an NTP server for the device, the device is synchronized to the NTP server, but the NTP server is not synchronized to the device.

Examples

Specify NTP server 10.1.1.1 for the device, and configure the device to run NTP version 4.

```
<Sysname> system-view
[Sysname] sntp unicast-server 10.1.1.1 version 4
```

Related commands

sntp authentication enable

sntp authentication-keyid

sntp reliable authentication-keyid

Contents

PoE commands

Only the PoE models support the PoE feature.

apply poe-profile

Use **apply poe-profile** to apply a PoE profile to a power interface (PI).

Use **undo apply poe-profile** to restore the default.

Syntax

apply poe-profile { **index** *index* | **name** *profile-name* }

undo apply poe-profile { **index** *index* | **name** *profile-name* }

Default

No PoE profile is applied to PIs.

Views

PI view

Predefined user roles

network-admin

Parameters

index *index*: Specifies a PoE profile by its index number in the range of 1 to 100.

name *profile-name*: Specifies a PoE profile by its name, a case-sensitive string of 1 to 15 characters.

Examples

Apply the PoE profile named **forIPphone** to GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] apply poe-profile name forIPphone
```

Related commands

apply poe-profile interface

display poe-profile

apply poe-profile interface

Use **apply poe-profile interface** to apply a PoE profile to PIs.

Use **undo apply poe-profile interface** to remove the PoE profile application from PIs.

Syntax

apply poe-profile { **index** *index* | **name** *profile-name* } **interface** *interface-range*

undo apply poe-profile { **index** *index* | **name** *profile-name* } **interface** *interface-range*

Default

No PoE profile is applied to a PI.

Views

System view

Predefined user roles

network-admin

Parameters

index *index*: Specifies a PoE profile by its index number in the range of 1 to 100.

name *profile-name*: Specifies a PoE profile by its name, a case-sensitive string of 1 to 15 characters.

interface-range: Specifies a range of Ethernet interfaces in the form of *interface-type interface-number* [**to** *interface-type interface-number*], where *interface-type interface-number* represents the interface type and interface number. The start interface number must be smaller than the end interface number. If an interface in the specified range does not support PoE, it is ignored when the PoE profile is applied.

Examples

Apply the PoE profile named **forIPphone** to GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] apply poe-profile name forIPphone interface gigabitethernet 1/0/1
```

Apply the PoE profile with index number 1 to PIs GigabitEthernet 1/0/2 to GigabitEthernet 1/0/6.

```
<Sysname> system-view
[Sysname] apply poe-profile index 1 interface gigabitethernet 1/0/2 to gigabitethernet
1/0/6
```

Related commands

apply poe-profile

display poe-profile interface

display poe device

Use **display poe device** to display general PSE information.

Syntax

display poe device [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, the command displays general PSE information about all PSEs in the IRF fabric.

Examples

Display general PSE information.

```
<Sysname> display poe device
Slot  1:
 PSE ID    Slot No.  SSlot No. PortNum   MaxPower(W)    State   Model
 4         1         0         48        600.0          Off     LSPPSE48A
```

Table 1 Command output

Field	Description
PSE ID	ID of the PSE.
Slot No.	Slot number of the PSE.
SSlot No.	Sub-slot number of the PSE.
PortNum	Number of PIs on the PSE.
MaxPower(W)	Maximum power of the PSE.
State	PSE status: • **On**—The PSE is supplying power. • **Off**—The PSE is not supplying power. • **Faulty**—The PSE has failed.
Model	PSE model.

display poe interface

Use **display poe interface** to display power supplying information for PIs.

Syntax

display poe interface [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays power supplying information for all PIs.

Examples

Display power supplying information for GigabitEthernet 1/0/1.

```
<Sysname> display poe interface gigabitethernet 1/0/1

 PoE Status                    : Enabled
 Power Priority                : Critical
 Oper                          : On
 IEEE Class                    : 1
 Detection Status              : Delivering power
 Power Mode                    : Signal
 Current Power                 : 11592   mW
 Average Power                 : 11610   mW
```

```
Peak Power                      : 11684    mW
Max Power                       : 15400    mW
Electric Current                : 244      mA
Voltage                         : 51.7     V
PD Description                  : IP Phone For Room 101
Legacy PD Detection             : Disabled
```

Table 2 Command output

Field	Description
PoE Status	PoE status: • Enabled. • Disabled.
Power Priority	Power supply priority: • Critical (highest). • High. • Low.
Oper	Operating status: • **Off**—PoE is disabled. • **On**—Power is being supplied to the PI correctly. • **Power-lack**—Remaining guaranteed power is insufficient for a critical PI. • **Power-deny**—The PSE refuses to supply power. The power required by the PD is higher than the configured power. • **Power-itself**—The PD is using another power supply. • **Power-limit**—The PSE is supplying power to the PD based on the configured power though the PD requires more power than the configured power.
IEEE Class	PD power class by which the PI supplies power to the PD. If the PI does not supplying power to the PD, this field displays a hyphen (-).
Detection Status	Power detection status: • **Disabled**—The PoE function is disabled. • **Searching**—The PI is searching for the PD. • **Delivering power**—The PI is supplying power to the PD. • **Fault**—A fault occurred during the test. • **Test**—The PI is undergoing a test. • **Other fault**—A fault has caused the PSE to enter the idle status. • **PD disconnected**—The PD is disconnected.
Power Mode	Power transmission mode: • **Signal**—Power is transmitted over the signal pairs of a twisted pair cable. • **Spare**—Power is transmitted over the spare pairs of a twisted pair cable.
Current Power	Current power, including PD consumption power and transmission loss.
Average Power	Average power.
Peak Power	Peak power.
Max Power	Maximum power.
Electric Current	Current.

Field	Description
Voltage	Voltage.
PD Description	Type and location description for the PD connected to the PI.

Display power supplying information for all PIs.

```
<Sysname> display poe interface
 Interface    PoE      Priority  CurPower  Oper    IEEE  Detection
                                 (W)               Class Status
 GE1/0/1      Disabled  Low      0.0       Off     0     Disabled
 GE1/0/2      Enabled   Low      0.0       Off     0     Searching
 GE1/0/3      Disabled  Low      0.0       Off     0     Disabled
 GE1/0/4      Disabled  Low      0.0       Off     0     Disabled
 GE1/0/5      Disabled  Low      0.0       Off     0     Disabled
 GE1/0/6      Disabled  Low      0.0       Off     0     Disabled
 GE1/0/7      Disabled  Low      0.0       Off     0     Disabled
 GE1/0/8      Disabled  Low      0.0       Off     0     Disabled
 GE1/0/9      Disabled  Low      0.0       Off     0     Disabled
 GE1/0/10     Disabled  Low      0.0       Off     0     Disabled
 GE1/0/11     Disabled  Low      0.0       Off     0     Disabled
 GE1/0/12     Disabled  Low      0.0       Off     0     Disabled
 GE1/0/13     Disabled  Low      0.0       Off     0     Disabled
 GE1/0/14     Disabled  Low      0.0       Off     0     Disabled
 GE1/0/15     Disabled  Low      0.0       Off     0     Disabled
 GE1/0/16     Disabled  Low      0.0       Off     0     Disabled
 GE1/0/17     Disabled  Low      0.0       Off     0     Disabled
 GE1/0/18     Disabled  Low      0.0       Off     0     Disabled
 GE1/0/19     Disabled  Low      0.0       Off     0     Disabled
 GE1/0/20     Disabled  Low      0.0       Off     0     Disabled
 GE1/0/21     Disabled  Low      0.0       Off     0     Disabled
 GE1/0/22     Disabled  Low      0.0       Off     0     Disabled
 GE1/0/23     Disabled  Low      0.0       Off     0     Disabled
 GE1/0/24     Disabled  Low      0.0       Off     0     Disabled
   ---  On State Ports: 0; Used: 0.0(W); Remaining: 370.0(W)  ---
```

Table 3 Command output

Field	Description
Interface	Interface name.
PoE	PoE status: • **Enabled**. • **Disabled**.
Priority	Power priority: • **Critical** (highest). • **High**. • **Low**.
CurPower	Current power of a PI.

Field	Description
Oper	Operating status: • **Off**—PoE is disabled. • **On**—Power is being supplied to the PI correctly. • **Power-lack**—Remaining guaranteed power is insufficient for a critical PI. • **Power-deny**—The PSE refuses to supply power. The power required by the PD is higher than the configured power. • **Power-itself**—The PD is using another power supply. • **Power-limit**—The PSE is supplying power to the PD based on the configured power though the PD requires more power than the configured power.
IEEE Class	PD power class by which the PI supplies power to the PD. If the PI does not supplying power to the PD, this field displays a hyphen (-).
Detection Status	Power detection status: • **Disabled**—PoE function is disabled. • **Searching**—The PI is searching for the PD. • **Delivering Power**—The PI is supplying power for the PD. • **Fault**—A fault occurred during the test. • **Test**—The PI is undergoing a test. • **Other fault**—A fault has caused the PSE to enter the idle status. • **PD disconnected**—The PD is disconnected.
On State Ports	Number of PIs that are supplying power.
Used	Power consumed by the current PI.
Remaining	(Devices that support dynamic power allocation.) Total remaining power of all PSEs configured with a maximum power. This field displays 0 if no PSE is configured with a maximum power (all PSEs participate in dynamic power allocation). (Devices that do not support dynamic power allocation.) Total remaining power of all PSEs.

display poe interface power

Use **`display poe interface power`** to display power information for PIs.

Syntax

`display poe interface power` [*`interface-type interface-number`*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

`interface-type interface-number`: Specifies an interface by its type and number. If you do not specify an interface, this command displays power information for all PIs.

Examples

Display power information for GigabitEthernet 1/0/1.

```
<Sysname> display poe interface power gigabitethernet 1/0/1
Interface    Current   Peak     Max      PD Description
             (W)       (W)      (W)
 GE1/0/1       15.0     15.3     30.0     Access Point on Room 509 for Peter
```

Display power information for all PIs.

```
<Sysname> display poe interface power
 Interface    Current   Peak     Max      PD Description
              (W)       (W)      (W)
 GE1/0/1      0.0       0.0      30.0
 GE1/0/2      0.0       0.0      30.0
 GE1/0/3      0.0       0.0      30.0
 GE1/0/4      0.0       0.0      30.0
 GE1/0/5      0.0       0.0      30.0
 GE1/0/6      0.0       0.0      30.0
 GE1/0/7      0.0       0.0      30.0
 GE1/0/8      0.0       0.0      30.0
 GE1/0/9      0.0       0.0      30.0
 GE1/0/10     0.0       0.0      30.0
 GE1/0/11     0.0       0.0      30.0
 GE1/0/12     0.0       0.0      30.0
 GE1/0/13     0.0       0.0      30.0
 GE1/0/14     0.0       0.0      30.0
 GE1/0/15     0.0       0.0      30.0
 GE1/0/16     0.0       0.0      30.0
 GE1/0/17     0.0       0.0      30.0
 GE1/0/18     0.0       0.0      30.0
 GE1/0/19     0.0       0.0      30.0
 GE1/0/20     0.0       0.0      30.0
 GE1/0/21     0.0       0.0      30.0
 GE1/0/22     0.0       0.0      30.0
 GE1/0/23     0.0       0.0      30.0
 GE1/0/24     0.0       0.0      30.0
   ---  On State Ports: 0; Used: 0.0(W); Remaining: 370.0(W)  ---
```

Table 4 Command output

Field	Description
Interface	Interface name.
CurPower	Current power.
PeakPower	Peak power.
MaxPower	Maximum power.
PD Description	Type and location description for the PD connected to a PI.
Ports On	Number of PIs that are supplying power.
Used	Power consumed by all PIs.

Field	Description
Remaining	(Devices that support dynamic power allocation.) Total remaining power of all PSEs configured with a maximum power. This field displays 0 if no PSE is configured with a maximum power (all PSEs participate in dynamic power allocation). (Devices that do not support dynamic power allocation.) Total remaining power of all PSEs.

display poe pse

Use **display poe pse** to display detailed PSE information.

Syntax

display poe pse [*pse-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

pse-id: Specifies a PSE by its ID. If you do not specify a PSE, this command displays detailed information about all PSEs.

Examples

Display detailed PSE information.

```
<Sysname> display poe pse
 PSE ID                        : 4
 Slot No.                      : 1
 SSlot No.                     : 0
 PSE Model                     : LSPPSE48A
 PSE Status                    : Enabled
 Power Priority                : Low
 Current Power                 : 0.0     W
 Average Power                 : 0.0     W
 Peak Power                    : 0.0     W
 Max Power                     : 600.0   W
 Max Allocable Power           : 600.0   W
 Remaining Guaranteed Power    : 600.0   W
 PSE CPLD Version              : -
 PSE Software Version          : 172
 PSE Hardware Version          : 0
 Legacy PD Detection           : Disabled
 Power Utilization Threshold   : 80
 PD Power Policy               : Priority
 PD Disconnect-Detection Mode  : DC
```

Table 5 Command output

Field	Description
PSE ID	ID of the PSE.
SSlot No.	Sublsot number of the PSE.
PSE Status	PoE status of the PSE: • Enabled. • Disabled.
PSE Fast Power Supply	PSE fast power supply enabling status: • Enabled. • Disabled.
Power Priority	Power priority of the PSE.
Current Power	Current power of the PSE.
Average Power	Average power of the PSE.
Peak Power	Peak power of the PSE.
Max Power	Maximum power of the PSE.
Max Allocable Power	Maximum allocable power of the PSE. (This field is supported only in Release 6340 and later.) The value of this field = Maximum power of the PSE – Sum of maximum powers of all PIs with forced PoE power supply enabled.
Remaining Guaranteed Power	Remaining guaranteed power of the PSE = Maximum guaranteed power of the PSE – Total maximum power of all critical PIs of the PSE.
PSE CPLD Version	PSE CPLD version number.
PSE Software Version	PSE software version number.
PSE Hardware Version	PSE hardware version number.
Legacy PD Detection	Nonstandard PD detection status: • Enabled. • Disabled.
Power Utilization Threshold	PSE power alarm threshold.
PD Power Policy	PD power management policy mode.
PD Disconnect-Detection Mode	PD disconnection detection mode.
PD High Inrush	Whether PD high inrush is enabled. • Enabled. • Disabled.

display poe pse interface

Use **display poe pse interface** to display the PoE status of all PIs on a PSE.

Syntax

display poe pse *pse-id* **interface**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

pse *pse-id*: Specifies a PSE ID. To display PSE ID and slot mappings, use the **display poe device** command.

Examples

Display the status of all PIs on PSE 4.

```
<Sysname> display poe pse 4 interface
 Interface   PoE      Priority  CurPower  Oper    IEEE  Detection
                                (W)               Class Status
 GE1/0/1     Disabled  Low      0.0       Off     0     Disabled
 GE1/0/2     Enabled   Low      0.0       Off     0     Searching
 GE1/0/3     Disabled  Low      0.0       Off     0     Disabled
 GE1/0/4     Disabled  Low      0.0       Off     0     Disabled
 GE1/0/5     Disabled  Low      0.0       Off     0     Disabled
 GE1/0/6     Disabled  Low      0.0       Off     0     Disabled
 GE1/0/7     Disabled  Low      0.0       Off     0     Disabled
 GE1/0/8     Disabled  Low      0.0       Off     0     Disabled
 GE1/0/9     Disabled  Low      0.0       Off     0     Disabled
 GE1/0/10    Disabled  Low      0.0       Off     0     Disabled
 GE1/0/11    Disabled  Low      0.0       Off     0     Disabled
 GE1/0/12    Disabled  Low      0.0       Off     0     Disabled
 GE1/0/13    Disabled  Low      0.0       Off     0     Disabled
 GE1/0/14    Disabled  Low      0.0       Off     0     Disabled
 GE1/0/15    Disabled  Low      0.0       Off     0     Disabled
 GE1/0/16    Disabled  Low      0.0       Off     0     Disabled
 GE1/0/17    Disabled  Low      0.0       Off     0     Disabled
 GE1/0/18    Disabled  Low      0.0       Off     0     Disabled
 GE1/0/19    Disabled  Low      0.0       Off     0     Disabled
 GE1/0/20    Disabled  Low      0.0       Off     0     Disabled
 GE1/0/21    Disabled  Low      0.0       Off     0     Disabled
 GE1/0/22    Disabled  Low      0.0       Off     0     Disabled
 GE1/0/23    Disabled  Low      0.0       Off     0     Disabled
 GE1/0/24    Disabled  Low      0.0       Off     0     Disabled
  ---  On State Ports: 0; Used: 0.0(W); Remaining: 370.0(W)  ---
```

Table 6 Command output

Field	Description
Interface	Interface name of a PI.
PoE	PoE status of a PI: • **Enabled**. • **Disabled**.

Field	Description
Priority	Priority of a PI: • **Critical** (highest). • **High**. • **Low**.
CurPower	Current power of a PI.
Oper	Operating status of a PI: • **Off**—PoE is disabled. • **On**—Power is being supplied to the PI correctly. • **Power-lack**—Remaining guaranteed power is insufficient for a critical PI. • **Power-deny**—The PSE refuses to supply power. The power required by the PD is higher than the configured power. • **Power-itself**—The PD is using another power supply. • **Power-limit**—The PSE is supplying power to the PD based on the configured power though the PD requires more power than the configured power.
IEEE Class	PD power class by which the PI supplies power to the PD. If the PI does not supplying power to the PD, this field displays a hyphen (-).
Detection Status	Power detection status of a PI: • **Disabled**—PoE function is disabled. • **Searching**—The PI is searching for the PD. • **Delivering Power**—The PI is supplying power to the PD. • **Fault**—A fault occurred during the test. • **Test**—The PI is undergoing a test. • **Other Fault**—A fault has caused the PSE to enter the idle status. • **PD Disconnected**—The PD is disconnected.
On State Ports	Number of PIs that are supplying power.
Used	Power consumed by PIs on the PSE.
Remaining	Remaining power of the PSE. This field displays 0 for a PSE that participates in dynamic power allocation.

display poe pse interface power

Use **`display poe pse interface power`** to display power information for PIs on a PSE.

Syntax

`display poe pse` *`pse-id`* **`interface power`**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

pse *pse-id*: Specifies a PSE by its ID. To display PSE ID and slot mappings, use the **display poe device** command.

Examples

Display power information for PIs on PSE 4.

```
<Sysname> display poe pse 4 interface power
 Interface    Current   Peak      Max      PD Description
              (W)       (W)       (W)
 GE1/0/1      0.0       0.0       30.0
 GE1/0/2      0.0       0.0       30.0
 GE1/0/3      0.0       0.0       30.0
 GE1/0/4      0.0       0.0       30.0
 GE1/0/5      0.0       0.0       30.0
 GE1/0/6      0.0       0.0       30.0
 GE1/0/7      0.0       0.0       30.0
 GE1/0/8      0.0       0.0       30.0
 GE1/0/9      0.0       0.0       30.0
 GE1/0/10     0.0       0.0       30.0
 GE1/0/11     0.0       0.0       30.0
 GE1/0/12     0.0       0.0       30.0
 GE1/0/13     0.0       0.0       30.0
 GE1/0/14     0.0       0.0       30.0
 GE1/0/15     0.0       0.0       30.0
 GE1/0/16     0.0       0.0       30.0
 GE1/0/17     0.0       0.0       30.0
 GE1/0/18     0.0       0.0       30.0
 GE1/0/19     0.0       0.0       30.0
 GE1/0/20     0.0       0.0       30.0
 GE1/0/21     0.0       0.0       30.0
 GE1/0/22     0.0       0.0       30.0
 GE1/0/23     0.0       0.0       30.0
 GE1/0/24     0.0       0.0       30.0
   ---  On State Ports: 0; Used: 0.0(W); Remaining: 370.0(W)  ---
```

Table 7 Command output

Field	Description
Interface	Interface name of a PI.
Current	Current power of a PI.
Peak	Peak power of a PI.
Max	Maximum power of a PI.
PD Description	Type and location description for the PD connected with a PI.
Ports On	Number of PIs that are supplying power.
Used	Power consumed by all PIs.
Remaining	Remaining power of the PSE. This field displays 0 for a PSE that participates in dynamic power allocation.

display poe-profile

Use **display poe-profile** to display information about the PoE profile.

Syntax

display poe-profile [**index** *index* | **name** *profile-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

index *index*: Specifies a PoE profile by its index number in the range of 1 to 100.

name *profile-name*: Specifies a PoE profile by its name, a case-sensitive string of 1 to 15 characters.

Usage guidelines

If you do not specify a profile, the command displays information about all PoE profiles.

Examples

Display information about all PoE profiles.

```
<Sysname> display poe-profile
 PoE Profile     Index   ApplyNum  Interfaces    Configuration
 forIPphone      1       4         GE1/0/1       poe enable
                                   GE1/0/2         poe priority critical
                                   GE1/0/3
                                   GE1/0/4
 forAP           2       2         GE1/0/5        poe enable
                                   GE1/0/6        poe max-power 14000
   ---  Total PoE profiles: 2, total ports: 6  ---
```

Display information about the PoE profile with index number 1.

```
<Sysname> display poe-profile index 1
 PoE Profile     Index   ApplyNum  Interfaces   Configuration
 forIPphone      1       6         GE1/0/1       poe enable
                                   GE1/0/2       poe priority critical
                                   GE1/0/3
                                   GE1/0/4
                                   GE1/0/5
                                   GE1/0/6
   ---  Total ports: 6  ---
```

Table 8 Command output

Field	Description
PoE Profile	Name of the PoE profile.
Index	Index number of the PoE profile.
ApplyNum	Number of PIs to which the PoE profile is applied.

Field	Description
Interfaces	Interface name of the PI to which the PoE configuration is applied.
Configuration	Configurations of the PoE profile.
Total PoE profiles	Number of PoE profiles.
Total ports	Number of PIs to which all PoE profiles are applied.

display poe-profile interface

Use **display poe-profile interface** to display information about the PoE profile on a PI.

Syntax

display poe-profile interface *interface-type interface-number*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Examples

Display information about the PoE profile on GigabitEthernet 1/0/1.

```
<Sysname> display poe-profile interface gigabitethernet 1/0/1
 PoEProfile     Index   ApplyNum  Interface   Effective configuration
 forIPphone      1       6        GE1/0/1       poe enable
                                                poe priority critical
```

The **Effective configuration** field displays the configurations that have taken effect. For the descriptions of other fields, see Table 8.

poe ai enable

Use **poe ai enable** to enable AI-driven PoE.

Use **undo ai poe enable** to disable AI-driven PoE.

Syntax

poe ai enable

undo poe ai enable

IMPORTANT:

This command is available only in Release 6318P01 and later.

Default

AI-driven PoE is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

With AI-driven PoE enabled, the device automatically recovers a PI when it fails. If more than one PI fails simultaneously, the device recovers the PIs one by one in ascending order of PI number.

AI-driven PoE automatically adjusts the power supply parameters to fit the power needs. If you disable AI-driven PoE, the system reverts the parameters to the settings before the adjustment.

AI-driven PoE takes effect only on PSEs that run firmware V147 or later.

- **Firmware earlier than V147**—You must use the **poe update** command to upgrade the PSE firmware and then enable AI-driven PoE on the PSE.
- **Firmware V147 or later**—You do not need to re-enable AI-driven PoE after upgrading the firmware if you have enabled the feature before the upgrade.

Examples

Enable AI-driven PoE.

```
<Sysname> system-view
[Sysname] poe ai enable
```

poe detection-mode

Use **poe detection-mode** to configure the PD detection mode.

Use **undo poe detection-mode** to restore the default.

Syntax

poe detection-mode { **none** | **simple** | **strict** }

undo poe detection-mode

Default

The default differs depending on the software version, as shown below:

Versions	Default setting
Versions earlier than Release 6350	The PD detection mode is **strict**.
Release 6350 and later	• If the device starts up with the initial configuration, the PD detection mode is **strict**. • If the device starts up with the factory defaults, the PD detection mode is **simple**.

Views

PI view

Predefined user roles

network-admin

Parameters

none: Enables the device to supply power to PDs that are correctly connected to the device without causing short circuit.

simple: Enables the device to supply power to PDs that comply with basic requirements of 802.3af or 802.3at.

strict: Enables the device to supply power to PDs that comply with all requirements of 802.3af or 802.3at.

Usage guidelines

CAUTION:

A non-PD device might be damaged when power is supplied to it. To avoid device damage, do not specify the **none** keyword when the PI connects to a non-PD device.

This command is available only for a PSE that has a model name ending with a character of **B**, **LSPPSE48B** for example. To obtain the model name of a PSE, execute the **display poe pse** command.

To configure the detection mode for nonstandard PDs, first execute the **poe legacy enable** command to enable detection for nonstandard PDs.

Examples

Configure the simple detection mode for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] poe detection-mode simple
```

Related commands

poe legacy enable

poe enable

Use **poe enable** to enable PoE on a PI.

Use **undo poe enable** to disable PoE on a PI.

Syntax

poe enable

undo poe enable

Default

- S5110V2 switch series:

  The default differs depending on the software version, as shown below:

Versions	Default setting
Versions earlier than Release 6328	PoE is disabled on PIs.
Release 6328 and later	• If the device starts up with the initial configuration, PoE is disabled on PIs. • If the device starts up with the factory defaults, PoE is enabled on PIs.

- S3100V3-SI switch series, S5130S-LI switch series, S5120V2-LI switch series, S5120V3-LI switch series, S5110V2-SI switch series, S5120V3-SI switch series, MS4300V2 switch series, MS4200 switch series, MS4320V2 switch series, MS4320V3 switch series, MS4320 switch series, WS5810-WiNet switch series, WS5820-WiNet switch series, S5000E-X switch series,

S5000X-EI switch series, S5000V3-EI switch series, S5000V5-EI switch series, and WAS6000 switch series:

PoE is enabled on PIs if the device starts up with the factory defaults and is disabled on PIs when the device starts up with the initial configuration.

For more information about the device initial configuration and factory defaults, see configuration file management in *Fundamentals Configuration Guide*.

Views

PI view

PoE profile view

Predefined user roles

network-admin

Usage guidelines

If a PoE profile has been applied to a PI, remove the application before configuring the PI in PoE profile view.

If a PI has been configured, remove the configuration before configuring the PI in PI view.

Examples

Enable PoE on a PI in PI view.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] poe enable
```

Enable PoE on a PI in PoE profile view.

```
<Sysname> system-view
[Sysname] poe-profile abc
[Sysname-poe-profile-abc-1] poe enable
```

Related commands

display poe interface

poe-profile

poe fast-on enable

Use **poe fast-on enable** to enable fast PoE for a PSE.

Use **undo poe fast-on enable** to disable fast PoE for the PSE.

IMPORTANT:
This command is supported only in Release 6328 and later.

Syntax

poe fast-on enable pse *pse-id*

undo poe fast-on enable pse *pse-id*

Default

Fast PoE is disabled on a PSE. PIs on the PSE supply power to PDs only after the PSE has started up.

Views

System view

Predefined user roles

network-admin

Parameters

pse *pse-id*: Specifies a PSE by its ID.

Usage guidelines

Fast PoE enables a PI on a PSE to supply power to PDs immediately after the PSE is powered on.

You must re-configure this command if you modified other PoE settings after configuring this command.

Examples

Enable fast PoE for PSE 4.

```
<Sysname> system-view
[Sysname] poe fast-on enable pse 4
```

Related commands

display poe pse

poe force-power

Use **poe force-power** to enable forced PoE power supply.

Use **undo poe force-power** to disable forced PoE power supply.

NOTE:

This command is supported only in Release 6340 and later.

Syntax

poe force-power

undo poe force-power

Default

Forced PoE power supply is disabled.

Views

PI view

Predefined user roles

network-admin

mdc-admin

Usage guidelines

CAUTION:

This command enables the device to supply power to a PD directly without performing a detection of the PD. To avoid damaging the PD, make sure the power provided by the device meets the PD specifications before executing this command.

Before supplying power to a PD, the device performs a detection of the PD. It supplies power to the PD only after the PD passes the detection. If the PD fails the detection but the power provided by the device meets the PD specifications, you can execute this command to enable forced power supply to the PD.

Examples

Enable forced PoE power supply.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] poe force-power
The PD might be damaged if the prowded by the device does not meet the PD power specifications.
Make sure you are fully aware of the impacts of this command when you use it in a live
network. Continue?[Y/N]: y
```

poe high-inrush enable

Use **poe high-inrush enable** to allow inrush currents drawn by PDs.

Use **undo poe high-inrush enable** to restore the default.

Syntax

poe high-inrush enable pse *pse-id*

undo poe high-inrush enable pse *pse-id*

Default

Inrush currents drawn by PDs are not allowed.

Views

System view

Predefined user roles

network-admin

Parameters

pse *pse-id*: Specifies a PSE by its ID.

Usage guidelines

CAUTION:

Inrush currents might damage the components on the device. Use this command with caution.

This command is available only for a PSE that has a model name ending with a character of **B**, **LSPPSE48B** for example. To obtain the model name of a PSE, execute the **display poe pse** command.

Inrush current might occur at PD startup and trigger PSE self-protection, As a result, the PSE stops supplying power to the PDs. To continue power supply to the PDs, configure this feature to allow inrush currents drawn by PDs.

IEEE 802.3af and IEEE 802.3at define specifications for inrush current. Support for the specifications defined by IEEE 802.3af and/or IEEE 802.3at depends on the device model.

Examples

All high inrush currents drawn by PDs.

```
<Sysname> system-view
[Sysname] poe high-inrush enable pse 4
```

Related commands

display poe interface

display poe pse

poe legacy enable (interface view)

Use **poe legacy enable** to enable nonstandard PD detection for a PI.

Use **undo poe legacy enable** to disable nonstandard PD detection for a PI.

Syntax

poe legacy enable

undo poe legacy enable

Default

Nonstandard PD detection is disabled for a PI.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

The device supports PSE-based and PI-based nonstandard PD detection. If you enable nonstandard PD detection both in system view and interface view, the configuration in system view takes effect.

As a best practice for disabling nonstandard PD detection for all PIs successfully in one operation, disable this feature in both system view and interface view.

Examples

Enable nonstandard PD detection for a PI.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] poe legacy enable
```

Related commands

display poe interface

poe legacy enable (system view)

poe legacy enable (system view)

Use **poe legacy enable** to enable the PSE to detect nonstandard PDs.

Use **undo poe legacy enable** to disable the PSE from detecting nonstandard PDs.

Syntax

poe legacy enable pse *pse-id*

undo poe legacy enable pse *pse-id*

Default

Nonstandard PD detection is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

pse *pse-id*: Specifies a PSE by its ID.

Usage guidelines

The device supports PSE-based and PI-based nonstandard PD detection. If you enable nonstandard PD detection both in system view and interface view, the configuration in system view takes effect.

As a best practice for disabling nonstandard PD detection for all PIs successfully in one operation, disable this feature in both system view and interface view.

Examples

Enable PSE 4 to detect nonstandard PDs.

```
<Sysname> system-view
[Sysname] poe legacy enable pse 4
```

Related commands

display poe pse

poe legacy enable (interface view)

poe max-power (interface view)

Use **poe max-power** to set the maximum PI power.

Use **undo poe max-power** to restore the default.

Syntax

poe max-power *max-power*

undo poe max-power

Default

The maximum PI power is 30000 W.

Views

PI view

PoE profile view

Predefined user roles

network-admin

Parameters

max-power: Sets the maximum PI power in milliwatts. The value range is 1000 to 30000.

Examples

Set the maximum PI power to 12000 milliwatts in PI view.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] poe max-power 12000
```

Set the maximum PI power to 12000 milliwatts in PoE profile view.

```
<Sysname> system-view
[Sysname] poe-profile abc
[Sysname-poe-profile-abc-1] poe max-power 12000
```

poe mps

Use **poe mps** to set the TMPDO for Maintain Power Signature (MPS).

Use **undo poe mps** to restore the default.

NOTE:

This command is supported only in R6350 and later.

Syntax

poe mps pse *pse-id* **tmpdo** { *timer* | **long** |**normal** }

undo poe mps pse *pse-id* **tmpdo**

Default

The normal TMPDO mode is used for the MPS. The TMPDO is 324 milliseconds.

Views

System view

Predefined user roles

network-admin

Parameters

pse-id: Specifies a PSE by its ID.

timer: Sets the TMPDO for the MPS. The value is a multiple of 4 in the range of 300 to 400, in milliseconds.

long: Specify the long TMPDO mode. The TMPDO is 360 milliseconds.

normal: Specifies the normal TMPDO mode. The TMPDO is 324 milliseconds.

Usage guidelines

The MPS is an electronic signature provided by a PD. The PD can use this signature to maintain connection to the PSE in sleep mode. The PD sends a PoE-compliant pulse current to the PSE periodically. If the PSE detects the PoE-compliant pulse current from the PD within the TMPDO, it supplies power to the PD. If the PSE does not detect the PoE-compliant pulse current from the PD within the TMPDO, it will not supply power to the PD.

To send pulse currents at larger intervals for lower standby power, you can use this command to change the TMPDO to be longer.

Only PSE modules that have a model name of LSPPSE**A support this feature. To view the PSE models, execute the **display poe pse** command.

If you execute the command multiple times, the most recent configuration takes effect.

Examples

Set the TMPDO for the MPS to 350 milliseconds.

```
<Sysname> system-view
[Sysname] poe mps pse 1 tmpdo 350
```

poe pd-description

Use **poe pd-description** to configure a description for the PD that connects to a PI.

Use **undo poe pd-description** to restore the default.

Syntax

poe pd-description *text*

undo poe pd-description

Default

No description is configured for the PD that connects to a PI.

Views

PI view

Predefined user roles

network-admin

Parameters

text: Configures a description for the PD connected to the PI, a case-sensitive string of 1 to 80 characters.

Examples

Configure the description for the PD as **IP Phone for Room 101**.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] poe pd-description IP Phone For Room 101
```

poe pd-policy priority

Use **poe pd-policy priority** to enable PI power management.

Use **undo poe pd-policy priority** to restore the default.

Syntax

poe pd-policy priority

undo poe pd-policy priority

Default

PI power management is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

If PI power management is disabled, the PSE does not supply power to new PDs when PSE power overload occurs.

If PI power management is enabled, when a PSE is overloaded, the PSE allocates power to PDs based on the priority of their PIs.

Examples

Enable PI power management.

```
<Sysname> system-view
[Sysname] poe pd-policy priority
```

Related commands

poe priority

poe priority (interface view)

Use **poe priority** to set the power supply priority for a PI.

Use **undo poe priority** to restore the default.

Syntax

poe priority { **critical** | **high** | **low** }

undo poe priority

Default

The power supply priority of a PI is **low**.

Views

PI view

PoE profile view

Predefined user roles

network-admin

Parameters

critical: Sets the power supply priority to **critical**. The PI with critical power priority operates in guaranteed mode. Power is first supplied to the PD connected to the critical PI.

high: Sets the power supply priority to **high**.

low: Sets the power supply priority to **low**.

Usage guidelines

When the PoE power is insufficient, power is first supplied to PIs with higher priority.

For PIs with same power supply priority, the PI with the smallest ID is allocated with power first.

If a PoE profile has been applied to a PI, remove the application before configuring the PI in PoE profile view.

If a PI has been configured, remove the configuration before configuring the PI in PI view.

Examples

Set the power supply priority of the PI to **critical** in PI view.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] poe priority critical
```

Set the power supply priority of the PI to **critical** in PoE profile view.

```
<Sysname> system-view
[Sysname] poe-profile abc
[Sysname-poe-profile-abc-1] poe priority critical
[Sysname-poe-profile-abc-1] quit
```

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] apply poe-profile name abc
```

Related commands

poe pd-policy priority

poe reset enable

Use **poe reset enable** to enable PI power cycling upon a system warm reboot.

Use **undo poe pse-policy priority** to disable PI power cycling upon a system warm reboot.

Syntax

poe reset enable

undo poe reset enable

Default

PI power cycling upon a system warm reboot is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

During the system warm reboot process (upon execution of the **reboot** command), the PIs continue supplying power to the PDs but data connections between the PDs and the device are interrupted. After the system reboots, PDs might not re-initiate data connections with the device. Power cycling PIs upon a system warm reboot allows the PDs to re-establish data connections with the device.

Examples

Enable PI power cycling upon a system warm reboot.

```
<Sysname> system-view
[Sysname] poe reset enable
```

poe track

Use **poe track** to associate a PI to a track entry.

Use **undo poe track** to restore the default.

NOTE:

This command is supported only in Release 6348P01 and later.

Syntax

poe track *track-entry-number* **action** { **alarm** | **alarm-reboot-pd** }

undo poe track

Default

A PI is not associated with any track entry.

Views

PI view

Predefined user roles

network-admin

Parameters

track-entry-number: Specify a track entry ID in the range of 1 to 1024.

action: Specifies the action to be taken when the track entry state changes from positive to negative.

alarm: Outputs an SNMP notification and log.

alarm-reboot-pd: Outputs an SNMP notification and log and reboots the PD connected to the PI.

Usage guidelines

This command uses a track entry to monitor the link status between the device and a PD and triggers the specified action when the track entry state changes from positive to negative. For more information about Track, see Track configuration in *High Availability Configuration Guide*.

If you configure this command multiple times in PI view, the most recent configuration takes effect.

Examples

Associate GigabitEthernet 1/0/1 with track entry 1 and enable the system to output an SNMP notification and log when the track entry state changes from positive to negative.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] poe track 1 action alarm
```

poe update

Use **poe update** to upgrade the PSE firmware when the device is operating.

Syntax

poe update { **full** | **refresh** } *filename* [**pse** *pse-id*]

Views

System view

Predefined user roles

network-admin

Parameters

full: Upgrades the PSE firmware in full mode.

refresh: Upgrades the PSE firmware in refresh mode.

filename: Specifies the name of the upgrade file, a case-insensitive string of 1 to 64 characters. The specified file must be in the root directory of the file system of the device.

pse *pse-id*: Specifies a PSE by its ID. If you do not specify a PSE, all PSEs are upgraded.

Usage guidelines

You can upgrade the PSE firmware in service in either of the following modes:

- **Refresh mode**—Updates the PSE firmware without deleting it. You can use the refresh mode in most cases.

- **Full mode**—Deletes the current PSE firmware and reloads a new one. Use the full mode if the PSE firmware is damaged and you cannot execute any PoE commands.

Examples

Upgrade the firmware of PSE 4 in service.

```
<Sysname> system-view
[Sysname] poe update refresh POE-168.bin pse 4
```

poe utilization-threshold

Use **poe utilization-threshold** to configure a power alarm threshold for the PSE.

Use **undo poe utilization-threshold** to restore the default power alarm threshold of the PSE.

Syntax

poe utilization-threshold *value* **pse** *pse-id*

undo poe utilization-threshold pse *pse-id*

Default

The power alarm threshold for the PSE is 80%.

Views

System view

Predefined user roles

network-admin

Parameters

value: Specifies alarm threshold as a percentage of 1 to 99.

pse *pse-id*: Specifies a PSE by its ID.

Usage guidelines

If PSE power usage crosses the threshold multiple times in succession, the system sends notification messages only for the first crossing. For more information, see "Configuring SNMP."

Examples

Set the power alarm threshold of PSE 4 to 90%.

```
<Sysname> system-view
[Sysname] poe utilization-threshold 90 pse 4
```

poe-profile

Use **poe-profile** to create a PoE profile and enter its view, or enter the view of an existing PoE profile.

Use **undo poe-profile** to delete a PoE profile.

Syntax

poe-profile *profile-name* [*index*]

undo poe-profile { **index** *index* | **name** *profile-name* }

Default

No PoE profiles exist.

Views

System view

Predefined user roles

network-admin

Parameters

profile-name: Specifies a PoE profile name, a case-sensitive string of 1 to 15 characters. A PoE configuration file name begins with a letter and must not contain reserved keywords including **undo**, **all**, **name**, **interface**, **user**, **poe**, **disable**, **max-power**, **mode**, **priority**, or **enable**.

index: Specifies the index number of a PoE profile, in the range of 1 to 100.

Usage guidelines

To configure PIs in batches, use the PoE profile.

If you do not specify a profile index, the system automatically assigns an index (starting from 1) to the PoE profile.

If a PoE profile is applied, use the **undo apply poe-profile** command to remove the application before deleting the PoE profile.

Examples

Create a PoE profile, name it **abc**, and specify the index number as **3**.

```
<Sysname> system-view
[Sysname] poe-profile abc 3
[Sysname-poe-profile-abc-3]
```

Create a PoE profile and name it **def**. Do not specify the index number.

```
<Sysname> system-view
[Sysname] poe-profile def
[Sysname-poe-profile-def-1]
```

Related commands

apply poe-profile

poe enable

poe max-power (interface view)

poe priority

Contents

SNMP commands

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

The SNMP agent sends notifications (traps and informs) to inform the NMS of significant events, such as link state changes and user logins or logouts. Unless otherwise stated, the **trap** keyword in the command line includes both traps and informs.

display snmp-agent community

Use **display snmp-agent community** to display information about SNMPv1 or SNMPv2c communities.

Syntax

display snmp-agent community [**read** | **write**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

read: Specifies SNMP read-only communities.

write: Specifies SNMP read and write communities.

Usage guidelines

This command is not available in FIPS mode.

If you do not specify the **read** or **write** keyword, this command displays information about all SNMPv1 and SNMPv2c communities.

SNMPv1 and SNMPv2c communities can be created in the following ways:

- Created by using the **snmp-agent community** command.
- Automatically created by the system for SNMPv1 and SNMPv2c users that have been assigned to an existing SNMP group.

This command displays information only about communities created and saved in plaintext form.

Examples

Display information about all SNMPv1 and SNMPv2c communities.

```
<Sysname> display snmp-agent community
   Community name: aa
       Group name: aa
       ACL:2001
       Storage-type: nonVolatile
       Context name: con1

   Community name: bb
       Role name: bb
```

```
       Storage-type: nonVolatile

   Community name: userv1
       Group name: testv1
       Storage-type: nonvolatile
Community name: cc
       Group name: cc
       ACL name: testacl
       Storage-type: nonVolatile
```

Table 1 Command output

Field	Description
Community name	Community name created by using the **snmp-agent community** command or username created by using the **snmp-agent usm-user { v1 | v2c }** command.
Group name	SNMP group name. • If the community is created by using the **snmp-agent community** command in VACM mode, the group name is the same as the community name. • If the community is created by using the **snmp-agent usm-user { v1 | v2c }** command, the name of the group that has the user is displayed.
Role name	User role name for the community. If the community is created by using the **snmp-agent community** command in RBAC mode, a user role can be bound to the community name.
ACL	Number of the ACL. This field appears only when an ACL is specified for the SNMPv1 or SNMPv2c community.
ACL name	Name of the ACL. This field appears only when an ACL is specified for the SNMPv1 or SNMPv2c community.
IPV6 ACL	Number of the IPv6 ACL. This field appears only when an ACL is specified for the SNMPv1 or SNMPv2c community.
IPV6 ACL name	Name of the IPv6 ACL. This field appears only when an ACL is specified for the SNMPv1 or SNMPv2c community.
Storage-type	Storage type: • **volatile**—Settings are lost when the system reboots. • **nonVolatile**—Settings remain after the system reboots. • **permanent**—Settings remain after the system reboots and can be modified but not deleted. • **readOnly**—Settings remain after the system reboots and cannot be modified or deleted. • **other**—Any other storage type.
Context name	SNMP context: • If a mapping between the SNMP community and an SNMP context is configured, the SNMP context is displayed. • If no mapping between the SNMP community and an SNMP context exists, this field is empty.

Related commands

snmp-agent community

snmp-agent usm-user { **v1** | **v2c** }

display snmp-agent context

Use **display snmp-agent context** to display SNMP contexts.

Syntax

display snmp-agent context [*context-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

context-name: Specifies an SNMP context by its name, a case-sensitive string of 1 to 32 characters. If you do not specify this argument, the command displays all SNMP contexts.

Examples

Display all SNMP contexts.

```
<Sysname> display snmp-agent context
   testcontext
```

Related commands

snmp-agent context

display snmp-agent group

Use **display snmp-agent group** to display information about SNMP groups.

Syntax

display snmp-agent group [*group-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group-name: Specifies an SNMPv1, SNMPv2c, or SNMPv3 group name in non-FIPS mode, and an SNMPv3 group name in FIPS mode. It is a case-sensitive string of 1 to 32 characters. If you do not specify a group, this command displays information about all SNMP groups.

Examples

Display information about all SNMP groups.

```
<Sysname> display snmp-agent group
   Group name: groupv3
```

```
Security model: v3 noAuthnoPriv
Readview: ViewDefault
Writeview: <no specified>
Notifyview: <no specified>
Storage-type: nonvolatile
 ACL name: testacl
```

Table 2 Command output

Field	Description
Group name	SNMP group name.
Security model	Security model of the SNMP group: • **authPriv**—Authentication with privacy. • **authNoPriv**—Authentication without privacy. • **noAuthNoPriv**—No authentication, no privacy. Security model of an SNMPv1 or SNMPv2c group can only be noAuthNoPriv.
Readview	Read-only MIB view accessible to the SNMP group.
Writeview	Write MIB view accessible to the SNMP group.
Notifyview	Notify MIB view for the SNMP group. The SNMP users in the group can send notifications only for the nodes in the notify MIB view.
Storage-type	Storage type, including **volatile**, **nonvolatile**, **permanent**, **readOnly**, and **other**. For more information, see Table 1.
ACL	Number of the IPv4 ACL. This field appears only when an IPv4 ACL is specified for the SNMP group.
ACL name	Name of the ACL. This field appears only when an ACL is specified for the SNMP group.
IPv6 ACL	Number of the IPv6 ACL. This field appears only when an IPv6 ACL is specified for the SNMP group.
IPV6 ACL name	Name of the IPv6 ACL. This field appears only when an IPv6 ACL is specified for the SNMP group.

Related commands

snmp-agent group

display snmp-agent local-engineid

Use **display snmp-agent local-engineid** to display the local SNMP engine ID.

Syntax

display snmp-agent local-engineid

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

Every SNMP entity has one SNMP engine to provide services for sending and receiving messages, authenticating and encrypting messages, and controlling access to managed objects.

An SNMP engine ID uniquely identifies an SNMP entity in an SNMP domain.

Examples

Display the local SNMP engine ID.

```
<Sysname> display snmp-agent local-engineid
   SNMP local engine ID: 800063A2800084E52BED7900000001
```

Related commands

snmp-agent local-engineid

display snmp-agent mib-node

Use **display snmp-agent mib-node** to display SNMP MIB node information.

Syntax

display snmp-agent mib-node [**details** | **index-node** | **trap-node** | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

details: Specifies detailed MIB node information, including node name, last octet of an OID string, and name of the next leaf node.

index-node: Specifies SNMP MIB tables, and node names and OIDs of MIB index nodes.

trap-node: Specifies node names and OIDs of MIB notification nodes, and node names and OIDs of notification objects.

verbose: Specifies detailed information about SNMP MIB nodes, including node names, OIDs, node types, permissions to MIB nodes, data types, MORs, and parent, child, and sibling nodes.

Usage guidelines

If you do not specify any keywords, this command displays information about all SNMP MIB nodes, including node name, OID, and permissions to MIB nodes.

The SNMP software package includes different MIB files. Support for MIBs varies by SNMP software versions.

Examples

Display SNMP MIB node information.

```
<Sysname> display snmp-agent mib-node

iso<1>(NA)
  |-std<1.0>(NA)
   |-iso8802<1.0.8802>(NA)
    |-ieee802dot1<1.0.8802.1>(NA)
     |-ieee802dot1mibs<1.0.8802.1.1>(NA)
```

```
...
```

Table 3 Command output

Field	Description
-std	MIB node name
<1.0>	MIB node OID
(NA)	Access right to the MIB node: • **NA**—Not accessible • **NF**—Notifications • **RO**—Read-only access • **RW**—Read and write access • **RC**—Read-write-create access • **WO**—Write-only access
*	Leaf node or MIB table node

Display detailed MIB node information.

```
<Sysname> display snmp-agent mib-node details

 iso(1)(dot1xPaeSystemAuthControl)
  |-std(0)(dot1xPaeSystemAuthControl)
   |-iso8802(8802)(dot1xPaeSystemAuthControl)
    |-ieee802dot1(1)(dot1xPaeSystemAuthControl)
     |-ieee802dot1mibs(1)(dot1xPaeSystemAuthControl)
      ...
```

Table 4 Command output

Field	Description
-std	MIB node name
(0)	Last bit of the MIB OID string
(lldpMessageTxInterval)	Name of the leaf node
*	Leaf node or MIB table node

Display MIB table names, and node names and OIDs of MIB index nodes.

```
<Sysname> display snmp-agent mib-node index-node

Table          |dot1xPaePortTable
Index          ||dot1xPaePortNumber
OID            |||  1.0.8802.1.1.1.1.1.2.1.1
...
```

Table 5 Command output

Field	Description
Table	MIB table name
Index	MIB index node name

Field	Description
OID	MIB index node OID

Display names and OIDs of MIB notification nodes, and names and OIDs of notification objects.

```
<Sysname> display snmp-agent mib-node trap-node


Name          |lldpRemTablesChange
OID           ||1.0.8802.1.1.2.0.0.1
Trap Object
Name          |||lldpStatsRemTablesInserts
OID           ||||1.0.8802.1.1.2.1.2.2
Name          |||lldpStatsRemTablesDeletes
OID           ||||1.0.8802.1.1.2.1.2.3
Name          |||lldpStatsRemTablesDrops
OID           ||||1.0.8802.1.1.2.1.2.4
Name          |||lldpStatsRemTablesAgeouts
OID           ||||1.0.8802.1.1.2.1.2.5
...
```

Table 6 Command output

Field	Description
Name	MIB notification node name
OID	MIB notification node OID
Trap Object	Name and OID of a notification object

Display detailed information about SNMP MIB nodes, including node names, OIDs, node types, permissions to MIB nodes, data types, MORs, and parent, child, and sibling nodes.

```
<Sysname> display snmp-agent mib-node verbose


Name          |iso
OID           ||1
Properties    ||NodeType:   Other
              ||AccessType: NA
              ||DataType:   NA
              ||MOR:        0x00000000
Parent        ||
First child   ||std
Next leaf     ||dot1xPaeSystemAuthControl
Next sibling  ||
...
```

Table 7 Command output

Field	Description
Name	MIB node name.
OID	MIB node OID.
Properties	MIB node properties.
NodeType	MIB node type: • **Table**—Table node. • **Row**—Row node in a MIB table. • **Column**—Column node in a MIB table. • **Leaf**—Leaf node. • **Group**—Group node (parent node of a leaf node). • **Trapnode**—Notification node. • **Other**—Other node type.
AccessType	Access right to the MIB node: • **NA**—Not accessible. • **NF**—Supports notifications. • **RO**—Supports read-only access. • **RW**—Supports read and write access. • **RC**—Supports read-write-create access. • **WO**—Supports write-only access.
DataType	Data type of the MIB node: • **Integer**—An integer. • **Integer32**—A 32-bit integer. • **Unsigned32**—A 32-bit integer with no mathematical sign. • **Gauge**—A non-negative integer that might increase or decrease. • **Gauge32**—A 32-bit non-negative integer that might increase or decrease. • **Counter**—A non-negative integer that might increase but not decrease. • **Counter32**—A 32-bit non-negative integer that might increase but not decrease. • **Counter64**—A 64-bit non-negative integer that might increase but not decrease. • **Timeticks**—A non-negative integer for time keeping. • **Octstring**—An octal string. • **OID**—Object identifier. • **IPaddress**—A 32-bit IP address. • **Networkaddress**—A network IP address. • **Opaque**—Any data. • **Userdefined**—User-defined data. • **BITS**—Bit enumeration. • **NA**—Other data type.
MOR	MOR for the MIB node.
Parent	Name of the parent node.
First child	Name of the first leaf node.
Next leaf	Name of the next leaf node.
Next sibling	Name of the next sibling node.

Field	Description
Allow	Operation types allowed: • **get/set/getnext**—All operations. • **get**—Get operation. • **set**—Set operation. • **getnext**—GetNext operation.
Value range	Value range of the MIB node.
Index	Table index. This field appears only for a table node.

display snmp-agent mib-view

Use **display snmp-agent mib-view** to display MIB views.

Syntax

display snmp-agent mib-view [**exclude** | **include** | **viewname** *view-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

exclude: Displays the subtrees excluded from any MIB view.

include: Displays the subtrees included in any MIB view.

viewname *view-name*: Displays information about the specified MIB view. The *view-name* argument is a case-sensitive string of 1 to 32 characters.

Usage guidelines

If you do not specify any parameters, this command displays all MIB views.

Examples

Display all MIB views.

```
<Sysname> display snmp-agent mib-view
   View name: ViewDefault
       MIB Subtree: iso
       Subtree mask:
       Storage-type: nonVolatile
       View Type: included
       View status: active

   View name: ViewDefault
       MIB Subtree: snmpUsmMIB
       Subtree mask:
       Storage-type: nonVolatile
       View Type: excluded
```

```
        View status: active

    View name: ViewDefault
        MIB Subtree: snmpVacmMIB
        Subtree mask:
        Storage-type: nonVolatile
        View Type: excluded
        View status: active

    View name: ViewDefault
        MIB Subtree: snmpModules.18
        Subtree mask:
        Storage-type: nonVolatile
        View Type: excluded
        View status: active
```

ViewDefault is the default MIB view. The output shows that except for the MIB objects in the **snmpUsmMIB**, **snmpVacmMIB**, and **snmpModules.18** subtrees, all the MIB objects in the **iso** subtree are accessible.

Table 8 Command output

Field	Description
View name	MIB view name.
MIB Subtree	MIB subtree covered by the MIB view.
Subtree mask	MIB subtree mask.
Storage-type	Type of the medium (see Table 1) where the subtree view is stored.
View Type	Access privilege for the MIB subtree in the MIB view: • **Included**—All objects in the MIB subtree are accessible in the MIB view. • **Excluded**—None of the objects in the MIB subtree is accessible in the MIB view.
View status	Status of the MIB view: • **active**—MIB view is effective. • **inactive**—MIB view is ineffective. The objects in the MIB view are not accessible, but they can send notifications.

Related commands

snmp-agent mib-view

display snmp-agent remote

Use **display snmp-agent remote** to display engine IDs of the remote SNMP entities.

Syntax

display snmp-agent remote [{ *ipv4-address* | **ipv6** *ipv6-address* }]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv4-address: Specifies a remote SNMP entity by its IPv4 address.

ipv6 *ipv6-address*: Specifies a remote SNMP entity by its IPv6 address.

Usage guidelines

Every SNMP entity has one SNMP engine to provide services for sending and receiving messages, authenticating and encrypting messages, and controlling access to managed objects.

An SNMP engine ID uniquely identifies an SNMP entity in an SNMP domain.

If you do not specify a remote SNMP entity, this command displays the engine IDs of all remote SNMP entities.

Examples

Display engine IDs of all remote SNMP entities.

```
<Sysname> display snmp-agent remote
   Remote engineID: 800063A28000A0FC00580400000001
       IPv4 address: 1.1.1.1
```

Table 9 Command output

Field	Description
Remote engineID	Remote SNMP engine ID you have configured using the **snmp-agent remote** command.
IPv4 address	IPv4 address of the remote SNMP entity.
IPv6 address	IPv6 address of the remote SNMP entity. This field is displayed if the remote SNMP entity is configured with an IPv6 address.

Related commands

snmp-agent remote

display snmp-agent statistics

Use **display snmp-agent statistics** to display SNMP message statistics.

Syntax

display snmp-agent statistics

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display SNMP message statistics.

```
<Sysname> display snmp-agent statistics
  1684 messages delivered to the SNMP entity.
  5 messages were for an unsupported version.
  0 messages used an unknown SNMP community name.
```

```
0 messages represented an illegal operation for the community supplied.
0 ASN.1 or BER errors in the process of decoding.
1679 messages passed from the SNMP entity.
0 SNMP PDUs had badValue error-status.
0 SNMP PDUs had genErr error-status.
0 SNMP PDUs had noSuchName error-status.
0 SNMP PDUs had tooBig error-status (Maximum packet size 1500).
16544 MIB objects retrieved successfully.
2 MIB objects altered successfully.
7 GetRequest-PDU accepted and processed.
7 GetNextRequest-PDU accepted and processed.
1653 GetBulkRequest-PDU accepted and processed.
1669 GetResponse-PDU accepted and processed.
2 SetRequest-PDU accepted and processed.
0 Trap PDUs accepted and processed.
0 alternate Response Class PDUs dropped silently.
0 forwarded Confirmed Class PDUs dropped silently.
```

Table 10 Command output

Field	Description
messages delivered to the SNMP entity	Number of messages that the SNMP agent has received.
messages were for an unsupported version	Number of messages that are not supported by the SNMP agent version.
messages used an unknown SNMP community name	Number of messages that used an unknown SNMP community name.
messages represented an illegal operation for the community supplied	Number of messages carrying an operation that the community has no right to perform.
ASN.1 or BER errors in the process of decoding	Number of messages that had ASN.1 or BER errors during decoding.
messages passed from the SNMP entity	Number of messages sent by the SNMP agent.
SNMP PDUs had badValue error-status	Number of PDUs with a BadValue error.
SNMP PDUs had genErr error-status	Number of PDUs with a genErr error.
SNMP PDUs had noSuchName error-status	Number of PDUs with a NoSuchName error.
SNMP PDUs had tooBig error-status	Number of PDUs with a TooBig error (the maximum packet size is 1500 bytes).
MIB objects retrieved successfully	Number of MIB objects that have been successfully retrieved.
MIB objects altered successfully	Number of MIB objects that have been successfully modified.
GetRequest-PDU accepted and processed	Number of GetRequest requests that have been received and processed.
GetNextRequest-PDU accepted and processed	Number of getNext requests that have been received and processed.
GetBulkRequest-PDU accepted and processed	Number of getBulk requests that have been received and processed.

Field	Description
GetResponse-PDU accepted and processed	Number of get responses that have been received and processed.
SetRequest-PDU accepted and processed	Number of set requests that have been received and processed.
Trap PDUs accepted and processed	Number of notifications that have been received and processed.
alternate Response Class PDUs dropped silently	Number of dropped response packets.
forwarded Confirmed Class PDUs dropped silently	Number of forwarded packets that have been dropped.

display snmp-agent sys-info

Use **display snmp-agent sys-info** to display SNMP agent system information.

Syntax

display snmp-agent sys-info [**contact** | **location** | **version**] *

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

contact: Displays the system contact.

location: Displays the physical location of the device.

version: Displays the SNMP agent version.

Usage guidelines

If you do not specify any keywords, this command displays all SNMP agent system information.

Examples

Display all SNMP agent system information.

```
<Sysname> display snmp-agent sys-info
   The contact information of the agent:
       New H3C Technologies Co., Ltd.

   The location information of the agent:
       Hangzhou, China

   The SNMP version of the agent:
       SNMPv3
```

Related commands

snmp-agent sys-info

display snmp-agent trap queue

Use **display snmp-agent trap queue** to display basic information about the trap queue.

Syntax

display snmp-agent trap queue

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the trap queue configuration and usage status.

```
<Sysname> display snmp-agent trap queue
   Queue size: 100
   Message number: 6
```

Related commands

snmp-agent trap life

snmp-agent trap queue-size

display snmp-agent trap-list

Use **display snmp-agent trap-list** to display SNMP notifications enabling status for modules.

Syntax

display snmp-agent trap-list

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

If a module has multiple sub-modules and SNMP notifications are enabled for one of its sub-modules, the command output shows that the module is SNMP notifications-enabled.

To determine whether a module supports SNMP notifications, execute the **snmp-agent trap enable ?** command.

The **display snmp-agent trap-list** command output varies by the **snmp-agent trap enable** command configuration and the module configuration.

Examples

Display SNMP notifications enabling status for modules.

```
<Sysname> display snmp-agent trap-list
   arp notification is disabled.
   configuration notification is enabled.
```

```
mac-address notification is enabled.
radius notification is disabled.
standard notification is enabled.
syslog notification is disabled.
system notification is enabled.

Enabled notifications: 4; Disabled notifications: 3
```

Related commands

snmp-agent trap enable

display snmp-agent usm-user

Use **display snmp-agent usm-user** to display SNMPv3 user information.

Syntax

display snmp-agent usm-user [**engineid** *engineid* | **group** *group-name* | **username** *user-name*] *

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

engineid *engineid*: Specifies an SNMP engine ID. The engine ID is case insensitive. When an SNMPv3 user is created, the system records the local SNMP entity engine ID. The user becomes invalid when the engine ID changes, and it becomes valid again when the recorded engine ID is restored.

group *group-name*: Specifies an SNMP group by its name. The group name is case sensitive.

username *user-name*: Specifies an SNMPv3 user by its name. The username is case sensitive.

Usage guidelines

This command displays only SNMPv3 users that you have created by using the **snmp-agent usm-user v3** command. To display SNMPv1 or SNMPv2c users created by using the **snmp-agent usm-user** { **v1** | **v2c** } command, use the **display snmp-agent community** command.

Examples

Display information about all SNMPv3 users.

```
<Sysname> display snmp-agent usm-user
   Username: userv3
   Group name: mygroupv3
       Engine ID: 800063A203000FE240A1A6
       Storage-type: nonVolatile
       UserStatus: active
       ACL: 2000

   Username: userv3
   Group name: mygroupv3
```

```
    Engine ID: 8000259503000BB3100A508
    Storage-type: nonVolatile
    UserStatus: active
    ACL name: testacl

Username: userv3code
Role name: groupv3code
           network-operator
    Engine ID: 800063A203000FE240A1A6
    Storage-type: nonVolatile
    UserStatus: active

Username: userv3code
Role name: snmprole
           network-operator
    Engine ID: 800063A280000002BB0001
    Storage-type: nonVolatile
    UserStatus: active
```

Table 11 Command output

Field	Description
Username	SNMP username.
Group name	SNMP group name.
Role name	SNMP user role name.
Engine ID	Engine ID that the SNMP agent used when the SNMP user was created.
Storage-type	Storage type: • **volatile**. • **nonvolatile**. • **permanent**. • **readOnly**. • **other**. For more information about these storage types, see Table 1.
UserStatus	SNMP user status: • **active**—The SNMP user is effective. • **notInService**—The SNMP user is correctly configured but not activated. • **notReady**—The SNMP user configuration is incomplete. • **other**—Any other status.
ACL	Number of the ACL. This field appears only when an ACL is specified for the SNMPv3 user.
ACL name	Name of the ACL. This field appears only when an ACL is specified for the SNMPv3 user.
IPV6 ACL	Number of the IPv6 ACL. This field appears only when an ACL is specified for the SNMPv3 user.
IPV6 ACL name	Name of the IPv6 ACL. This field appears only when an ACL is specified for the SNMPv3 user.

Related commands

snmp-agent usm-user v3

enable snmp trap updown

Use **enable snmp trap updown** to enable link state notifications on an interface.

Use **undo enable snmp trap updown** to disable link state notifications on an interface.

Syntax

enable snmp trap updown

undo enable snmp trap updown

Default

Link state notifications are enabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

For an interface to generate linkUp/linkDown notifications when its state changes, you must also enable the linkUp/linkDown notification function globally by using the **snmp-agent trap enable standard** [**linkdown** | **linkup**] * command.

Examples

Enable GigabitEthernet 1/0/1 to send linkUp/linkDown SNMP traps to 10.1.1.1 in the community **public**.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable
[Sysname] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname
public
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] enable snmp trap updown
```

Related commands

snmp-agent target-host

snmp-agent trap enable

snmp-agent

Use **snmp-agent** to enable the SNMP agent.

Use **undo snmp-agent** to disable the SNMP agent.

Syntax

snmp-agent

undo snmp-agent

Default

On the following switches, the SNMP agent is disabled.

- S5110V2 switch series
- S5110V2-SI switch series
- S5120V2-LI switch series
- S5130S-LI switch series
- S3100V3-SI switch series
- S5120V3-SI switch series
- S5120V3-LI switch series
- MS4320V3 switch series
- MS4320V2 switch series
- MS4320 switch series
- MS4200 switch series
- MS4300V2 switch series

On the following switches, the SNMP agent is enabled when the switch starts up with factory defaults and is disabled when the switch starts up with the initial configuration. For more information about the device initial configuration and factory defaults, see configuration file management in *Fundamentals Configuration Guide*.

- S5000V3-EI switch series
- S5000V5-EI switch series
- WS5810-WiNet switch series
- WS5820-WiNet switch series
- S5000E-X switch series
- S5000X-EI switch series
- WAS6000 switch series

Views

System view

Predefined user roles

network-admin

Usage guidelines

The SNMP agent is automatically enabled when you execute any command that begins with **snmp-agent** except for the **snmp-agent calculate-password** command.

The SNMP agent will fail to be enabled when the port that the agent will listen on is used by another service. You can use the **snmp-agent port** command to specify a listening port. To view the UDP port use information, execute the **display udp verbose** command.

If you disable the SNMP agent, the SNMP settings do not take effect. The **display current-configuration** command does not display the SNMP settings. The SNMP settings will not be saved in the configuration file. For the SNMP settings to take effect, enable the SNMP agent.

Examples

Enable the SNMP agent.

```
<Sysname> system-view
[Sysname] snmp-agent
```

Related commands

display udp verbose (see IP performance optimization commands in *Layer 3—IP Services Configuration Guide*)

snmp-agent port

snmp-agent { inform | trap } source

Use **snmp-agent** { **inform** | **trap** } **source** to specify a source IP address for the informs or traps sent by the SNMP agent.

Use **undo snmp-agent** { **inform** | **trap** } **source** to restore the default.

Syntax

snmp-agent { **inform** | **trap** } **source** *interface-type interface-number*

undo snmp-agent { **inform** | **trap** } **source**

Default

The SNMP agent uses the IP address of the outgoing interface as the source IP address of notifications.

Views

System view

Predefined user roles

network-admin

Parameters

inform: Specifies informs.

trap: Specifies traps.

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

The **snmp-agent source** command enables the SNMP agent to use the primary IP address of an interface or subinterface as the source IP address in all its SNMP informs or traps, regardless of their outgoing interfaces. An NMS can use this IP address to filter all the informs or traps sent by the SNMP agent.

Make sure the specified interface has been created and assigned a valid IP address. The configuration will fail if the interface has not been created and will take effect only after a valid IP address is assigned to the specified interface.

Examples

Configure the primary IP address of GigabitEthernet 1/0/1 as the source address of SNMP traps.

```
<Sysname> system-view
[Sysname] snmp-agent trap source gigabitethernet 1/0/1
```

Configure the primary IP address of GigabitEthernet 1/0/2 as the source address of SNMP informs.

```
<Sysname> system-view
[Sysname] snmp-agent inform source gigabitethernet 1/0/2
```

Related commands

snmp-agent target-host

snmp-agent trap enable

snmp-agent calculate-password

Use **snmp-agent calculate-password** to calculate the encrypted form for a key in plaintext form.

Syntax

In non-FIPS mode:

snmp-agent calculate-password *plain-password* **mode** { **3desmd5** | **3dessha** | **aes192md5** | **aes192sha** | **aes256md5** | **aes256sha** | **md5** | **sha** } { **local-engineid** | **specified-engineid** *engineid* }

In FIPS mode:

snmp-agent calculate-password *plain-password* **mode** { **aes192sha** | **aes256sha** | **sha** } { **local-engineid** | **specified-engineid** *engineid* }

Views

System view

Predefined user roles

network-admin

Parameters

plain-password: Specifies a key in plaintext form. The *plain-password* argument is a case-sensitive string of 1 to 64 characters.

mode: Specifies an authentication algorithm and encryption algorithm. The device supports the HMAC-MD5 and HMAC-SHA1 authentication algorithms. The HMAC-MD5 algorithm is faster than the HMAC-SHA1 algorithm. The HMAC-SHA1 algorithm provides more security than the HMAC-MD5 algorithm. The AES256, AES192, AES, 3DES, and DES encryption algorithms (in descending order of security strength) are available for the device. A more secure algorithm calculates slower. DES is enough to meet general security requirements.

- **3desmd5**: Calculates the encrypted form for the encryption key by using the 3DES encryption algorithm and HMAC-MD5 authentication algorithm.
- **3dessha**: Calculates the encrypted form for the encryption key by using the 3DES encryption algorithm and HMAC-SHA1 authentication algorithm.
- **aes192md5**: Calculates the encrypted form for the encryption key by using the AES192 encryption algorithm and the HMAC-MD5 authentication algorithm.
- **aes192sha**: Calculates the encrypted form for the encryption key by using the AES192 encryption algorithm and the HMAC-SHA1 authentication algorithm.
- **aes256md5**: Calculates the encrypted form for the encryption key by using the AES256 encryption algorithm and the HMAC-MD5 authentication algorithm.
- **aes256 sha**: Calculates the encrypted form for the encryption key by using the AES256 encryption algorithm and the HMAC-SHA1 authentication algorithm.
- **md5**: Calculates the encrypted form for the authentication key or encryption key by using the HMAC-MD5 authentication algorithm and AES or DES encryption algorithm. When the HMAC-MD5 authentication algorithm is used, you can get the same authentication key or encryption key in encrypted form regardless of whether the AES or DES encryption algorithm is used.
- **sha**: Calculates the encrypted form for the authentication key or encryption key by using HMAC-SHA1 authentication algorithm and AES or DES encryption algorithm. When the HMAC-SHA1 authentication algorithm is used, you can get the same authentication key or encryption key in encrypted form regardless of whether the AES or DES encryption algorithm is used.

local-engineid: Uses the local engine ID to calculate the encrypted form for the key. You can configure the local engine ID by using the **snmp-agent local-engineid** command.

specified-engineid *engineid*: Uses a user-defined engine ID to calculate the encrypted form for the key. The *engineid* argument is an even number of case-insensitive hexadecimal characters. All-zero and all-F strings are invalid. The even number is in the range of 10 to 64.

Usage guidelines

Make sure the SNMP agent is enabled before you execute the **snmp-agent calculate-password** command.

For security purposes, use the encrypted-form key generated by using this command when you create SNMPv3 users by specifying the **cipher** keyword in the **snmp-agent usm-user v3** command.

The encrypted form of the key is valid only under the engine ID specified for key conversion.

Examples

Use the local engine ID and the HMAC-SHA1 algorithm to calculate the encrypted form for key **authkey**.

```
<Sysname> system-view
[Sysname] snmp-agent calculate-password authkey mode sha local-engineid
The encrypted key is: 09659EC5A9AE91BA189E5845E1DDE0CC
```

Related commands

snmp-agent local-engineid

snmp-agent usm-user v3

snmp-agent community

Use **snmp-agent community** to configure an SNMPv1 or SNMPv2c community.

Use **undo snmp-agent community** to delete an SNMPv1 or SNMPv2c community.

Syntax

In VACM mode:

snmp-agent community { **read** | **write** } [**simple** | **cipher**] *community-name* [**mib-view** *view-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

undo snmp-agent community [**cipher**] *community-name*

In RBAC mode:

snmp-agent community [**simple** | **cipher**] *community-name* **user-role** *role-name* [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

undo snmp-agent community [**cipher**] *community-name*

Default

No SNMPv1 or SNMPv2c communities exist.

Views

System view

Predefined user roles

network-admin

Parameters

read: Assigns the specified community read-only access to MIB objects. A read-only community can only inquire MIB information.

write: Assigns the specified community read and write access to MIB objects. A read and write community can configure MIB information.

simple: Specifies a community name in plaintext form. For security purposes, the community name specified in plaintext form will be stored in encrypted form.

cipher: Specifies a community name in encrypted form.

community-name: Specifies the community name. The plaintext form is a case-sensitive string of 1 to 32 characters. The encrypted form is a case-sensitive string of 33 to 73 characters. Input a string as escape characters after a backslash (\).

mib-view *view-name*: Specifies the MIB view available for the community. The *view-name* argument represents a MIB view name, a case-sensitive string of 1 to 32 characters. A MIB view represents a set of accessible MIB objects. If you do not specify a view, the specified community can access the MIB objects in the default MIB view **ViewDefault**.

user-role *role-name*: Specifies a user role name for the community, a case-sensitive string of 1 to 63 characters.

acl: Specifies a basic or advanced IPv4 ACL for the community.

ipv4-acl-number: Specifies a basic or advanced IPv4 ACL by its number. The basic IPv4 ACL number is in the range of 2000 to 2999. The advanced IPv4 ACL number is in the range of 3000 to 3999.

name *ipv4-acl-name*: Specifies a basic or advanced IPv4 ACL by its name, a case-insensitive string of 1 to 63 characters.

acl ipv6: Specifies a basic or advanced IPv6 ACL for the community.

ipv6-acl-number: Specifies a basic or advanced IPv6 ACL by its number. The basic IPv6 ACL number is in the range of 2000 to 2999. The advanced IPv6 ACL number is in the range of 3000 to 3999.

name *ipv6-acl-name*: Specifies a basic or advanced IPv6 ACL by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

This command is not available in FIPS mode.

Only users with the network-admin or level-15 user role can execute this command. Users with other user roles cannot execute this command even if these roles are granted access to commands of the SNMP feature or this command.

An SNMP community is identified by a community name. It contains a set of NMSs and SNMP agents. Devices in an SNMP community authenticate each other by using the community name. An NMS and an SNMP agent can communicate only when they use the same community name.

Typically, **public** is used as the read-only community name and **private** is used as the read and write community name. To enhance security, you can assign your SNMP communities a name other than **public** and **private**.

The **snmp-agent community** command allows you to use either of the following modes to control SNMP community access to MIB objects:

- **View-based access control model**—The VACM mode controls access to MIB objects by assigning MIB views to SNMP communities.
- **Role based access control**—The RBAC mode controls access to MIB objects by assigning user roles to SNMP communities.

-
- The network-admin and level-15 user roles have the read and write access to all MIB objects.
- The network-operator user role has the read-only access to all MIB objects.

For more information about user roles, see *Fundamentals Configuration Guide*.

RBAC mode controls access on a per MIB object basis, and VACM mode controls access on a MIB view basis. As a best practice to enhance MIB security, use RBAC mode.

You can create a maximum of 10 SNMP communities by using the **snmp-agent community** command.

If you execute the command multiple times to specify the same community name but different other settings each time, the most recent configuration takes effect.

To set and save a community name in plain text, do not specify the **simple** or **cipher** keyword.

The ACL is used to filter illegitimate NMSs.

- If you do not specify an ACL, the specified ACL does not exist, or the specified ACL does not have any rules, all NMSs that use the community name can access the SNMP agent.
- If you specify an ACL and the ACL has rules, only NMSs permitted by the ACL can access the SNMP agent.

For more information about ACL, see *ACL and QoS Configuration Guide*.

You can also create an SNMP community by using the **snmp-agent usm-user** { **v1** | **v2c** } and **snmp-agent group** { **v1** | **v2c** } commands. These two commands create an SNMPv1 or SNMPv2c user and the group to which the user is assigned. The system automatically creates an SNMP community by using the SNMPv1 or SNMPv2c username.

The **display snmp-agent community** command displays information only about communities created and saved in plaintext form.

Examples

Create the read-only community with the plaintext form name **readaccess** so an SNMPv1 or SNMPv2c NMS can use the community name **readaccess** to read the MIB objects in the default view **ViewDefault**.

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v1 v2c
[Sysname] snmp-agent community read simple readaccess
```

Create the read and write community with the plaintext form name **writeaccess** so only the SNMPv2c NMS at 1.1.1.1 can use the community name **writeaccess** to read or set the MIB objects in the default view **ViewDefault**.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0.0.0.0
[Sysname-acl-ipv4-basic-2001] rule deny source any
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent community write simple writeaccess acl 2001
```

Create the read and write community with the plaintext form name **writeaccess** so only the SNMPv2c NMS at 1.1.1.2 can use the community name **writeaccess** to read or set the MIB objects in the default view **ViewDefault**.

```
<Sysname> system-view
[Sysname] acl basic name testacl
[Sysname-acl-ipv4-basic-testacl] rule permit source 1.1.1.2 0.0.0.0
```

```
[Sysname-acl-ipv4-basic-testacl] rule deny source any
[Sysname-acl-ipv4-basic-testacl] quit
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent community write simple writeaccess acl name testacl
```

Create the read and write community with the plaintext form name **wr-sys-acc** so an SNMPv1 or SNMPv2c NMS can use the community name **wr-sys-acc** to read or set the MIB objects in the system subtree (OID 1.3.6.1.2.1.1).

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v1 v2c
[Sysname] undo snmp-agent mib-view ViewDefault
[Sysname] snmp-agent mib-view included test system
[Sysname] snmp-agent community write simple wr-sys-acc mib-view test
```

Related commands

display snmp-agent community

snmp-agent mib-view

snmp-agent community-map

Use **snmp-agent community-map** to map an SNMP community to an SNMP context.

Use **undo snmp-agent community-map** to delete the mapping between an SNMP community and an SNMP context.

Syntax

snmp-agent community-map *community-name* **context** *context-name*

undo snmp-agent community-map *community-name* **context** *context-name*

Default

No mapping exists between an SNMP community and an SNMP context.

Views

System view

Predefined user roles

network-admin

Parameters

community-name: Specifies an SNMP community, a case-sensitive string of 1 to 32 characters.

context-name: Specifies an SNMP context, a case-sensitive string of 1 to 32 characters.

Usage guidelines

This command enables a module on an agent to obtain the context mapped to a community name when an NMS accesses the agent by using SNMPv1 or SNMPv2c.

You can configure a maximum of 10 community-context mappings on the device.

Examples

Map SNMP community **private** to SNMP context **trillcontext**.

```
<Sysname> system-view
[Sysname] snmp-agent community-map private context testcontext
```

Related commands

display snmp-agent community

snmp-agent configuration-examine interval

Use **snmp-agent configuration-examine interval** to set the intervals at which the SNMP module examines the system configuration for changes.

Use **undo snmp-agent configuration-examine interval** to restore the default.

NOTE:

This command is supported only in Release 6340 and later.

Syntax

snmp-agent configuration-examine interval *interval*

undo snmp-agent configuration-examine interval

Default

The SNMP module examines the system configuration for changes at intervals of 600 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the intervals at which the SNMP module examines the system configuration for changes, in seconds. The value range for this argument is 1 to 86400.

Usage guidelines

The SNMP module examines the system running configuration, startup configuration, and next-startup configuration file for changes periodically and generates a log if any change is found. If SNMP notification for configuration changes has been enabled, the system generates also an SNMP notification.

You can use this command to modify the examination interval.

Examples

Set the intervals at which the SNMP module examines the system configuration for changes to 600 seconds.

```
<sysname> system-view
[sysname] snmp-agent configuration-examine interval 600
```

Related commands

snmp-agent trap enable

snmp-agent context

Use **snmp-agent context** to create an SNMP context.

Use **undo snmp-agent context** to delete an SNMP context.

Syntax

snmp-agent context *context-name*

undo snmp-agent context *context-name*

Default

No SNMP contexts exist.

Views

System view

Predefined use roles

network-admin

Parameters

context-name: Specifies an SNMP context, a case-sensitive string of 1 to 32 characters.

Usage guidelines

For an NMS and an SNMP agent to communicate, configure the same SNMP context for them or do not configure a context for the NMS.

You can create a maximum of 20 SNMP contexts.

Examples

Create SNMP context **trillcontext**.

```
<Sysname> system-view
[Sysname] snmp-agent context testcontext
```

Related commands

display snmp-agent context

snmp-agent group

Use **snmp-agent group** to create an SNMP group.

Use **undo snmp-agent group** to delete an SNMP group.

Syntax

In non-FIPS mode:

- SNMPv1 and SNMP v2c:

  snmp-agent group { **v1** | **v2c** } *group-name* [**notify-view** *view-name* | **read-view** *view-name* | **write-view** *view-name*] * [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

  undo snmp-agent group { **v1** | **v2c** } *group-name*

- SNMPv3:

  snmp-agent group v3 *group-name* [**authentication** | **privacy**] [**notify-view** *view-name* | **read-view** *view-name* | **write-view** *view-name*] * [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

  undo snmp-agent group v3 *group-name* [**authentication** | **privacy**]

In FIPS mode:

snmp-agent group v3 *group-name* { **authentication** | **privacy** } [**notify-view** *view-name* | **read-view** *view-name* | **write-view** *view-name*] * [**acl**

{ *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

undo snmp-agent group v3 *group-name* { **authentication** | **privacy** }

Default

No SNMP groups exist.

Views

System view

Predefined use roles

network-admin

Parameters

v1: Specifies SNMPv1.

v2c: Specifies SNMPv2c.

v3: Specifies SNMPv3.

group-name: Specifies an SNMP group name, a case-sensitive string of 1 to 32 characters.

authentication: Specifies the authentication without privacy security model for the SNMPv3 group.

privacy: Specifies the authentication with privacy security model for the SNMPv3 group.

read-view *view-name*: Specifies a read-only MIB view. The *view-name* represents a MIB view name, a case-sensitive string of 1 to 32 characters. If you do not specify a read-only MIB view, the SNMP group has read access to the default view **ViewDefault**.

notify-view *view-name*: Specifies a notify MIB view. The *view-name* represents a MIB view name, a case-sensitive string of 1 to 32 characters. The SNMP agent sends notifications to the users in the specified group only for the MIB objects included in the notify view. If you do not specify a notify view, the SNMP agent does not send any notification to the users in the specified group.

write-view *view-name:* Specifies a read and write MIB view. The *view-name* represents a MIB view name, a case-sensitive string of 1 to 32 characters. If you do not specify a read and write view, the SNMP group cannot set any MIB object on the SNMP agent.

acl: Specifies a basic or advanced IPv4 ACL for the group.

ipv4-acl-number: Specifies a basic or advanced IPv4 ACL by its number. The basic IPv4 ACL number is in the range of 2000 to 2999. The advanced IPv4 ACL number is in the range of 3000 to 3999.

name *ipv4-acl-name*: Specifies a basic or advanced IPv4 ACL by its name, a case-insensitive string of 1 to 63 characters.

acl ipv6: Specifies a basic or advanced IPv6 ACL for the group.

ipv6-acl-number: Specifies a basic or advanced IPv6 ACL by its number. The basic IPv6 ACL number is in the range of 2000 to 2999. The advanced IPv6 ACL number is in the range of 3000 to 3999.

name *ipv6-acl-name*: Specifies a basic or advanced IPv6 ACL by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

SNMPv1 and SNMPv2c settings in this command are not supported in FIPS mode.

Only users with the network-admin or level-15 user role can execute this command. Users with other user roles cannot execute this command even if these roles are granted access to commands of the SNMP feature or this command.

All users in an SNMP group share the security model and access rights of the group.

You can create a maximum of 20 SNMP groups, including SNMPv1, SNMPv2c, and SNMPv3 groups.

All SNMPv3 users in a group share the same security model, but can use different authentication and encryption key settings. To implement a security model for a user and avoid SNMP communication failures, make sure the security model configuration for the group and the security key settings for the user are compliant with Table 12 and match the settings on the NMS.

Table 12 Basic security setting requirements for different security models

Security model	Security model keyword for the group	Security key settings for the user	Remarks
Authentication with privacy	**privacy**	Authentication key, encryption key	If the authentication key or the encryption key is not configured, SNMP communication will fail.
Authentication without privacy	**authentication**	Authentication key	If no authentication key is configured, SNMP communication will fail. The encryption key (if any) for the user does not take effect.
No authentication, no privacy	Neither **authentication** nor **privacy**	None	The authentication and encryption keys, if configured, do not take effect.

You can specify an ACL for the user and group, respectively, to filter illegitimate NMSs. Only the NMSs permitted by the ACLs for both the user and group can access the SNMP agent. The following rules apply to the ACLs for the user and group:

- If you do not specify an ACL, the specified ACL does not exist, or the specified ACL does not have any rules, all NMSs that use the username can access the SNMP agent.
- If you have specified an ACL and the ACL has rules, only the NMSs permitted by the ACL can access the agent.

For more information about ACL, see *ACL and QoS Configuration Guide*.

Examples

Create the SNMPv3 group **group1**.

```
<Sysname> system-view
[Sysname] snmp-agent group v3 group1
```

Related commands

display snmp-agent group

snmp-agent mib-view

snmp-agent usm-user

snmp-agent local-engineid

Use **snmp-agent local-engineid** to set an SNMP engine ID.

Use **undo snmp-agent local-engineid** to restore the default.

Syntax

snmp-agent local-engineid *engineid*

undo snmp-agent local-engineid

Default

The engine ID of a device is the combination of the company ID and the device ID.

Views

System view

Predefined user roles

network-admin

Parameters

engineid: Specifies an SNMP engine ID, a case-insensitive hexadecimal string. Its length is an even number in the range of 10 to 64. All-zero and all-F strings are invalid.

Usage guidelines

An SNMP engine ID uniquely identifies a device in an SNMP managed network. Make sure the local SNMP engine ID is unique within your SNMP managed network to avoid communication problems.

If you have configured SNMPv3 users, change the local SNMP engine ID only when necessary. The change can void the SNMPv3 usernames and encrypted keys you have configured.

You can use the default engine ID or configure an easy-to-remember engine ID based on the network plan. For example, you can set the engine ID for device 1 on the first floor of building A to 000Af0010001 and device 2 to 000Af0010002.

Examples

Set the local SNMP engine ID to **123456789A**.

```
<Sysname> system-view
[Sysname] snmp-agent local-engineid 123456789A
```

Related commands

display snmp-agent local-engineid

snmp-agent usm-user

snmp-agent log

Use **snmp-agent log** to enable SNMP logging.

Use **undo snmp-agent log** to disable SNMP logging.

Syntax

snmp-agent log { **all** | **authfail** | **get-operation** | **set-operation** }

undo snmp-agent log { **all** | **authfail** | **get-operation** | **set-operation** }

Default

SNMP logging operations are disabled.

Views

System view

Predefined user roles

network-admin

Parameters

all: Enables logging SNMP authentication failures, Get operations, and Set operations.

authfail: Enables logging SNMP authentication failures.

get-operation: Enables logging SNMP Get operations.

set-operation: Enables logging SNMP Set operations.

Usage guidelines

Use SNMP logging to record the SNMP operations performed on the SNMP agent or authentication failures from the NMS to the agent for auditing NMS behaviors. The SNMP agent sends log data to the information center. You can configure the information center to output the data to a destination as needed.

Examples

Enable logging SNMP Get operations.

```
<Sysname> system-view
[Sysname] snmp-agent log get-operation
```

Enable logging SNMP Set operations.

```
<Sysname> system-view
[Sysname] snmp-agent log set-operation
```

Enable logging SNMP authentication failures.

```
<Sysname> system-view
[Sysname] snmp-agent log authfail
```

snmp-agent mib-view

Use **snmp-agent mib-view** to create or update a MIB view.

Use **undo snmp-agent mib-view** to delete a MIB view.

Syntax

snmp-agent mib-view { **excluded** | **included** } *view-name oid-tree* [**mask** *mask-value*]

undo snmp-agent mib-view *view-name*

Default

The system creates the **ViewDefault** view when the SNMP agent is enabled. In this default MIB view, all MIB objects in the **iso** subtree but the **snmpUsmMIB**, **snmpVacmMIB**, and **snmpModules.18** subtrees are accessible.

Views

System view

Predefined user roles

network-admin

Parameters

excluded: Denies access to any node in the specified MIB subtree.

included: Permits access to all the nodes in the specified MIB subtree.

view-name: Specifies a view name, a case-sensitive string of 1 to 32 characters.

oid-tree: Specifies a MIB subtree by its root node's OID (for example, **1.3.6.1.2.1.1**) or object name (for example, **system**). The *oid-tree* argument is a case-sensitive string of 1 to 255 characters. An OID is a dotted numeric string that uniquely identifies an object in the MIB tree.

mask *mask-value*: Sets a MIB subtree mask, a case-insensitive hexadecimal string. Its length is an even number in the range of 1 to 32.

Usage guidelines

A MIB view represents a set of MIB objects (or MIB object hierarchies) with certain access privilege. The MIB objects included in the MIB view are accessible while those excluded from the MIB view are inaccessible.

Each *view-name oid-tree* pair represents a view record. If you specify the same record with different MIB subtree masks multiple times, the most recent configuration takes effect.

Be cautious with deleting the default MIB view. The operation blocks the access to any MIB object on the device from NMSs that use the default view.

Examples

Include the **mib-2** (OID 1.3.6.1.2.1) subtree in the **mibtest** view and exclude the **system** subtree from this view.

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v1
[Sysname] snmp-agent mib-view included mibtest 1.3.6.1.2.1
[Sysname] snmp-agent mib-view excluded mibtest system
[Sysname] snmp-agent community read public mib-view mibtest
```

An SNMPv1 NMS in the **public** community can query the objects in the **mib-2** subtree but not any object (for example, the **sysDescr or sysObjectID** node) in the **system** subtree.

Related commands

display snmp-agent mib-view

snmp-agent group

snmp-agent packet max-size

Use **snmp-agent packet max-size** to set the maximum size (in bytes) of SNMP packets that an SNMP agent can receive or send.

Use **undo snmp-agent packet max-size** to restore the default.

Syntax

snmp-agent packet max-size *byte-count*

undo snmp-agent packet max-size

Default

An SNMP agent can process SNMP packets with a maximum size of 1500 bytes.

Views

System view

Predefined user roles

network-admin

Parameters

byte-count: Sets the maximum size (in bytes) of SNMP packets that the SNMP agent can receive or send. The value range is 484 to 17940.

Usage guidelines

If any device on the path to the NMS does not support packet fragmentation, limit the SNMP packet size to prevent large-sized packets from being discarded. For most networks, the default value is sufficient.

Examples

Set the maximum SNMP packet size to 1024 bytes.

```
<Sysname> system-view
[Sysname] snmp-agent packet max-size 1024
```

snmp-agent packet response dscp

Use **snmp-agent packet response dscp** to set the DSCP value for SNMP responses.

Use **undo snmp-agent packet response dscp** to restore the default.

Syntax

snmp-agent packet response dscp *dscp-value*

undo snmp-agent packet response dscp

Default

The DSCP value for SNMP responses is 0.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Sets the DSCP value for SNMP responses, in the range of 0 to 63. A greater DSCP value represents a higher priority.

Usage guidelines

The DSCP value is encapsulated in the ToS field of an IP packet. It specifies the priority level of the packet for transmission.

Examples

Set the DSCP value to 40 for SNMP responses.

```
<Sysname> system-view
[Sysname] snmp-agent packet response dscp 40
```

snmp-agent port

Use **snmp-agent port** to specify an SNMP listening port.

Use **undo snmp-agent port** to restore the default.

Syntax

snmp-agent port *port-number*

undo snmp-agent port

Default

The SNMP listening port is UDP port 161.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies an SNMP listening port by its number in the range of 1 to 65535.

Usage guidelines

The SNMP agent will fail to be enabled when the port that the agent will listen on is used by another service. You can use the **snmp-agent port** command to change the SNMP listening port. As a best practice, execute the **display udp verbose** command to view the UDP port use information before specifying a new SNMP listening port.

After changing the SNMP listening port, the NMS can perform SNMP set and get operations on the device only after reconnecting the device by using the new port number.

Examples

Specify **5555** as the SNMP listening port..

```
<Sysname> system-view
[Sysname] snmp-agent port 5555
```

Related commands

display udp verbose (see IP performance optimization commands in *Layer 3—IP Services Configuration Guide*)

snmp-agent remote

Use **snmp-agent remote** to set an SNMP engine ID for a remote SNMP entity.

Use **undo snmp-agent remote** to delete the SNMP engine ID of a remote SNMP entity.

Syntax

snmp-agent remote { *ipv4-address* | **ipv6** *ipv6-address* } **engineid** *engineid*

undo snmp-agent remote *ip-address*

Default

No SNMP engine IDs are configured for remote SNMP entities.

Views

System view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies a remote SNMP entity by its IPv4 address.

ipv6 *ipv6-address*: Specifies a remote SNMP entity by its IPv6 address.

engineid: Specifies the SNMP engine ID of the remote SNMP entity. This argument is a case-insensitive hexadecimal string. Its length is an even number in the range of 10 to 64. All-zero and all-F strings are invalid.

Usage guidelines

To send informs to an NMS, you must configure the SNMP engine ID of the NMS on the SNMP agent.

The NMS accepts the SNMPv3 informs from the SNMP agent only if the engine ID in the informs is the same as its local engine ID.

You can configure a maximum of 20 remote SNMP engine IDs.

Examples

Set the SNMP engine ID to **123456789A** for the remote entity **10.1.1.1**.

```
<Sysname> system-view
[Sysname] snmp-agent remote 10.1.1.1 engineid 123456789A
```

Related commands

display snmp-agent remote

snmp-agent sys-info contact

Use **snmp-agent sys-info contact** to configure the system contact.

Use **undo snmp-agent sys-info contact** to restore the default contact.

Syntax

snmp-agent sys-info contact *sys-contact*

undo snmp-agent sys-info contact

Default

The system contact is **New H3C Technologies Co., Ltd.**.

Views

System view

Predefined user roles

network-admin

Parameters

sys-contact: Specifies the system contact, a case-sensitive string of 1 to 255 characters.

Usage guidelines

Configure the system contact for system maintenance and management.

Examples

Configure the system contact as **Dial System Operator # 27345**.

```
<Sysname> system-view
[Sysname] snmp-agent sys-info contact Dial System Operator # 27345
```

Related commands

display snmp-agent sys-info

snmp-agent sys-info location

Use **snmp-agent sys-info location** to configure the system location.

Use **undo snmp-agent sys-info location** to restore the default location.

Syntax

snmp-agent sys-info location *sys-location*

undo snmp-agent sys-info location

Default

The system location is **Hangzhou, China**.

Views

System view

Predefined user roles

network-admin

Parameters

sys-location: Specifies the system location, a case-sensitive string of 1 to 255 characters.

Usage guidelines

Configure the location of the device for system maintenance and management.

Examples

Configure the system location as **Room524-row1-3**.

```
<Sysname> system-view
[Sysname] snmp-agent sys-info location Room524-row1-3
```

Related commands

display snmp-agent sys-info

snmp-agent sys-info version

Use **snmp-agent sys-info version** to enable SNMP versions.

Use **undo snmp-agent sys-info version** to disable SNMP versions.

Syntax

In non-FIPS mode:

snmp-agent sys-info contact version { **all** | { **v1** | **v2c** | **v3** } * }

undo snmp-agent sys-info version { **all** | { **v1** | **v2c** | **v3** } * }

In FIPS mode:

snmp-agent sys-info version v3

undo snmp-agent sys-info version v3

Default

SNMPv3 is enabled.

Views

System view

Predefined user roles

network-admin

Parameters

all: Specifies SNMPv1, SNMPv2c, and SNMPv3.

v1: Specifies SNMPv1.

v2c: Specifies SNMPv2c.

v3: Specifies SNMPv3.

Usage guidelines

SNMPv1 and SNMPv2c settings in this command are not supported in FIPS mode.

Configure the SNMP agent with the same SNMP version as the NMS for successful communications between them.

To use SNMP notifications in IPv6, enable SNMPv2c or SNMPv3.

Examples

Enable SNMPv3.

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v3
```

Related commands

display snmp-agent sys-info

snmp-agent target-host

Use **snmp-agent target-host** to configure an SNMP notification target host.

Use **undo snmp-agent target-host** to remove an SNMP notification target host.

Syntax

In non-FIPS mode:

snmp-agent target-host inform address udp-domain { *ipv4-target-host* | **ipv6** *ipv6-target-host* } [**udp-port** *port-number*] **params securityname** *security-string* { **v2c** | **v3** [**authentication** | **privacy**] }

snmp-agent target-host trap address udp-domain { *ipv4-target-host* | **ipv6** *ipv6-target-host* } [**udp-port** *port-number*] [**dscp** *dscp-value*] **params securityname** *security-string* [**v1** | **v2c** | **v3** [**authentication** | **privacy**]]

undo snmp-agent target-host { **trap** | **inform** } **address udp-domain** { *ipv4-target-host* | **ipv6** *ipv6-target-host* } **params securityname** *security-string*

In FIPS mode:

snmp-agent target-host inform address udp-domain { *ipv4-target-host* | **ipv6** *ipv6-target-host* } [**udp-port** *port-number*] **params securityname** *security-string* **v3** { **authentication** | **privacy** }

snmp-agent target-host trap address udp-domain { *ipv4-target-host* | **ipv6** *ipv6-target-host* } [**udp-port** *port-number*] [**dscp** *dscp-value*] **params securityname** *security-string* **v3** { **authentication** | **privacy** }

undo snmp-agent target-host { **trap** | **inform** } **address udp-domain** { *ipv4-target-host* | **ipv6** *ipv6-target-host* } **params securityname** *security-string*

Default

No SNMP notification target hosts exist.

Views

System view

Predefined user roles

network-admin

Parameters

inform: Specifies a host that receives informs.

trap: Specifies a host that receives traps.

address: Specifies the destination address of SNMP notifications.

udp-domain: Specifies UDP as the transport protocol.

ipv4-target-host: Specifies a target host by its IPv4 address or host name. The host name is a case-insensitive string of 1 to 253 characters. The string can only contain letters, numbers, hyphens (-), underscores (_), and dots (.). If you specify a host name, the IPv4 address of the target host can be obtained.

ipv6 *ipv6-target-host*: Specifies a target host by its IPv6 address or host name. The host name is a case-insensitive string of 1 to 253 characters, which only contains letters, numbers, hyphens (-), underscores (_), and dots (.). If you specify a host name, the IPv6 address of the target host can be obtained. If you specify an IPv6 address, the address cannot be a link local address.

udp-port *port-number*: Specifies the UDP port for SNMP notifications. The default port number is 162.

dscp-value: Sets the DSCP value for traps sent to the target host, in the range of 0 to 63. The DSCP value is encapsulated in the ToS field of an IP packet. It specifies the priority level of the packet and affects the transmission priority of the packet. A greater DSCP value represents a higher priority. The default DSCP value for traps is 0.

params securityname *security-string*: Specifies the authentication parameter. The *security-string* argument specifies an SNMPv1 or SNMPv2c community name or an SNMPv3 username, a case-sensitive string of 1 to 32 characters.

v1: Specifies SNMPv1.

v2c: Specifies SNMPv2c.

v3: Specifies SNMPv3.

- **authentication**: Specifies the security model to be authentication without privacy. You must specify the authentication key when you create the SNMPv3 user.
- **privacy**: Specifies the security model to be authentication with privacy. You must specify the authentication key and encryption key when you create the SNMPv3 user.

Usage guidelines

You can specify multiple SNMP notification target hosts.

Make sure the SNMP agent uses the same UDP port for SNMP notifications as the target host. Typically, NMSs, for example, IMC and MIB Browser, use port 162 for SNMP notifications as defined in the SNMP protocols.

If none of the keywords **v1**, **v2c**, or **v3** is specified, SNMPv1 is used. Make sure the SNMP agent uses the same SNMP version as the target host so the host can receive the notification.

If neither **authentication** nor **privacy** is specified, the security model is no authentication, no privacy.

Examples

Configure the SNMP agent to send SNMPv3 traps to 10.1.1.1 by using the username **public**.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable standard
```

```
[Sysname] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname
public v3
```

Related commands

snmp-agent { **inform** | **trap** } **source**

snmp-agent trap enable

snmp-agent trap life

snmp-agent trap enable

Use **snmp-agent trap enable** to enable SNMP notifications.

Use **undo snmp-agent trap enable** to disable SNMP notifications.

Syntax

snmp-agent trap enable [**configuration** | *protocol* | **standard** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**] * | **system**]

undo snmp-agent trap enable [**configuration** | *protocol* | **standard** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**] * | **system**]

Default

SNMP configuration notifications, standard notifications, and system notifications are enabled. Whether other SNMP notifications are enabled varies by module.

Views

System view

Predefined user roles

network-admin

Parameters

configuration: Specifies configuration notifications. If configuration notifications are enabled, the system checks the running configuration and the startup configuration every 10 minutes for any change and generates a notification for the most recent change.

protocol: Specifies protocol module notifications. You can use the **snmp-agent trap enable ?** command to obtain the value of this argument. For more information about this argument, see the command reference for each module.

standard: Specifies SNMP standard notifications.

Table 13 Standard SNMP notifications

Keyword	Definition
authentication	Authentication failure notification sent when an NMS fails to be authenticated by the SNMP agent.
coldstart	Notification sent when the device restarts.
linkdown	Notification sent when the link of a port goes down.
linkup	Notification sent when the link of a port comes up.
warmstart	Notification sent when the SNMP agent restarts.

system: Specifies system notifications sent when the system time is modified, the system reboots, or the main system software image is not available.

Usage guidelines

To report critical protocol events to an NMS, first enable the protocol and then enable SNMP notifications for the protocol.

To use SNMP notifications in IPv6, enable SNMPv2c or SNMPv3.

For SNMP notifications to be sent correctly, you must also configure the notification sending parameters as required.

If no optional parameters are specified, this command or its **undo** form enables or disables all SNMP notifications supported by the device.

Examples

Enable the SNMP agent to send SNMP authentication failure notifications.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable standard authentication
```

Related commands

snmp-agent sys-info version

snmp-agent target-host

snmp-agent trap if-mib link extended

Use **snmp-agent trap if-mib link extended** to configure the SNMP agent to send extended linkUp/linkDown notifications.

Use **undo snmp-agent trap if-mib link extended** to restore the default.

Syntax

snmp-agent trap if-mib link extended

undo snmp-agent trap if-mib link extended

Default

The SNMP agent sends standard linkUp/linkDown notifications.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Extended linkUp and linkDown notifications add interface description and interface type to the standard linkUp/linkDown notifications for fast failure point identification.

When you use this command, make sure the NMS supports the extended linkup and linkDown notifications.

Examples

Enable extended linkUp/linkDown notifications.

```
<Sysname> system-view
[Sysname] snmp-agent trap if-mib link extended
```

snmp-agent trap life

Use **snmp-agent trap life** to set the lifetime of notifications in the SNMP notification queue.

Use **undo snmp-agent trap life** to restore the default notification lifetime.

Syntax

snmp-agent trap life *seconds*

undo snmp-agent trap life

Default

The SNMP notification lifetime is 120 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

seconds: Sets a lifetime in the range of 1 to 2592000, in seconds.

Usage guidelines

When congestion occurs, the SNMP agent buffers notifications in a queue. The notification lifetime sets how long a notification can stay in the queue. A notification is deleted when its lifetime expires.

Examples

Set the SNMP notification lifetime to 60 seconds.

```
<Sysname> system-view
[Sysname] snmp-agent trap life 60
```

Related commands

snmp-agent target-host

snmp-agent trap enable

snmp-agent trap queue-size

snmp-agent trap log

Use **snmp-agent trap log** to enable SNMP notification logging.

Use **undo snmp-agent trap log** to disable SNMP notification logging.

Syntax

snmp-agent trap log

undo snmp-agent trap log

Default

SNMP notification logging is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Use SNMP notification logging to record SNMP notifications sent by the SNMP agent for notification tracking. The SNMP agent sends the logs to the information center. You can configure the information center to output the logs to a destination as needed.

Examples

Enable SNMP notification logging.

```
<Sysname> system-view
[Sysname] snmp-agent trap log
```

snmp-agent trap queue-size

Use **snmp-agent trap queue-size** to set the SNMP notification queue size.

Use **undo snmp-agent trap queue-size** to restore the default queue size.

Syntax

snmp-agent trap queue-size *size*

undo snmp-agent trap queue-size

Default

The SNMP notification queue can store a maximum of 100 notifications.

Views

System view

Predefined user roles

network-admin

Parameters

size: Specifies the maximum number of notifications that the SNMP notification queue can hold. The value range is 1 to 1000.

Usage guidelines

When congestion occurs, the SNMP agent buffers notifications in a queue. SNMP notification queue size sets the maximum number of notifications that this queue can hold.

When the queue size is reached, the system discards the new notification it receives.

If modification of the queue size causes the number of notifications in the queue to exceed the queue size, the oldest notifications are dropped for new notifications.

Examples

Set the SNMP notification queue size to 200.

```
<Sysname> system-view
[Sysname] snmp-agent trap queue-size 200
```

Related commands

snmp-agent target-host

snmp-agent trap enable

snmp-agent trap life

snmp-agent usm-user { v1 | v2c }

Use **snmp-agent usm-user { v1 | v2c }** to create an SNMPv1 or SNMPv2c user.

Use **undo snmp-agent usm-user { v1 | v2c }** to delete an SNMPv1 or SNMPv2c user.

Syntax

snmp-agent usm-user { **v1** | **v2c** } *user-name group-name* [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

undo snmp-agent usm-user { **v1** | **v2c** } *user-name*

Default

No SNMPv1 or SNMPv2c users exist.

Views

System view

Predefined user roles

network-admin

Parameters

v1: Specifies SNMPv1.

v2c: Specifies SNMPv2c.

user-name: Specifies an SNMP username, a case-sensitive string of 1 to 32 characters.

group-name: Specifies an SNMPv1 or SNMPv2c group name, a case-sensitive string of 1 to 32 characters. The group can be one that has been created or not. The user takes effect only after you create the group.

acl: Specifies a basic or advanced IPv4 ACL for the user.

ipv4-acl-number: Specifies a basic or advanced IPv4 ACL by its number. The basic IPv4 ACL number is in the range of 2000 to 2999. The advanced IPv4 ACL number is in the range of 3000 to 3999.

name *ipv4-acl-name*: Specifies a basic or advanced IPv4 ACL by its name, a case-insensitive string of 1 to 63 characters.

acl ipv6: Specifies a basic or advanced IPv6 ACL for the user.

ipv6-acl-number: Specifies a basic or advanced IPv6 ACL by its number. The basic IPv6 ACL number is in the range of 2000 to 2999. The advanced IPv6 ACL number is in the range of 3000 to 3999.

name *ipv6-acl-name*: Specifies a basic or advanced IPv6 ACL by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

This command is not available in FIPS mode.

Only users with the network-admin or level-15 user role can execute this command. Users with other user roles cannot execute this command even if these roles are granted access to commands of the SNMP feature or this command.

On an SNMPv1 or SNMPv2c network, NMSs and agents authenticate each other by using the community name. On an SNMPv3 network, NMSs and agents authenticate each other by using the username.

You can create an SNMPv1 or SNMPv2c community by using either of the following ways:

- Execute the **snmp-agent community** command.
- Execute the **snmp-agent usm-user** { **v1** | **v2c** } and **snmp-agent group** { **v1** | **v2c** } commands to create an SNMPv1 or SNMPv2c user and the group that the user is assigned to. The system automatically creates an SNMP community by using the SNMPv1 or SNMPv2c username.

The **display snmp-agent community** command displays information only about communities created and saved in plaintext form.

You can specify an ACL for the user and group, respectively, to filter illegitimate NMSs. Only the NMSs permitted by the ACLs for both the user and group can access the SNMP agent. The following rules apply to the ACLs for the user and group:

- If you do not specify an ACL, the specified ACL does not exist, or the specified ACL does not have any rules, all NMSs that use the username can access the SNMP agent.
- If you have specified an ACL and the ACL has rules, only the NMSs permitted by the ACL can access the agent.

For more information about ACL, see *ACL and QoS Configuration Guide*.

Examples

Add the user **userv2c** to the SNMPv2c group **readCom** so an NMS can use the protocol SNMPv2c and the read-only community name **userv2c** to access the device.

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent group v2c readCom
[Sysname] snmp-agent usm-user v2c userv2c readCom
```

Add the user **userv2c** in the SNMPv2c group **readCom** so only the NMS at 1.1.1.1 can use the protocol SNMPv2c and read-only community name **userv2c** to access the device.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0.0.0.0
[Sysname-acl-ipv4-basic-2001] rule deny source any
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent group v2c readCom
[Sysname] snmp-agent usm-user v2c userv2c readCom acl 2001
```

Add the user **userv2c** in the SNMPv2c group **readCom** so only the NMS at 1.1.1.2 can use the protocol SNMPv2c and read-only community name **userv2c** to access the device.

```
[Sysname] acl basic name testacl
[Sysname-acl-ipv4-basic-testacl] rule permit source 1.1.1.2 0.0.0.0
[Sysname-acl-ipv4-basic-testacl] rule deny source any
[Sysname-acl-ipv4-basic-testacl] quit
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent group v2c readCom
[Sysname] snmp-agent usm-user v2c userv2c readCom acl name testacl
```

Related commands

display snmp-agent community

snmp-agent community

snmp-agent group

snmp-agent usm-user v3

Use **snmp-agent usm-user v3** to create an SNMPv3 user.

Use **undo snmp-agent usm-user v3** to delete an SNMPv3 user.

Syntax

In non-FIPS mode:

- In VACM mode:

  snmp-agent usm-user v3 *user-name group-name* [**remote** { *ipv4-address* | **ipv6** *ipv6-address* }] [{ **cipher** | **simple** } **authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **3des** | **aes128** | **aes192** | **aes256** | **des56** } *priv-password*]] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

  undo snmp-agent usm-user v3 *user-name* { **local** | **engineid** *engineid-string* | **remote** { *ipv4-address* | **ipv6** *ipv6-address* } }

- In RBAC mode:

  snmp-agent usm-user v3 *user-name* **user-role** *role-name* [**remote** { *ipv4-address* | **ipv6** *ipv6-address* }] [{ **cipher** | **simple** } **authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **3des** | **aes128** | **aes192** | **aes256** | **des56** } *priv-password*]] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

  undo snmp-agent usm-user v3 *user-name* { **local** | **engineid** *engineid-string* | **remote** { *ipv4-address* | **ipv6** *ipv6-address* } }

In FIPS mode:

- In VACM mode:

  snmp-agent usm-user v3 *user-name group-name* [**remote** { *ipv4-address* | **ipv6** *ipv6-address* }] { **cipher** | **simple** } **authentication-mode sha** *auth-password* [**privacy-mode** { **aes128** | **aes192** | **aes256** } *priv-password*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

  undo snmp-agent usm-user v3 *user-name* { **local** | **engineid** *engineid-string* | **remote** { *ipv4-address* | **ipv6** *ipv6-address* } }

- In RBAC mode:

  snmp-agent usm-user v3 *user-name* **user-role** *role-name* [**remote** { *ipv4-address* | **ipv6** *ipv6-address* }] [{ **cipher** | **simple** } **authentication-mode sha** *auth-password* [**privacy-mode** { **aes128** | **aes192** | **aes256** } *priv-password*]] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

  undo snmp-agent usm-user v3 *user-name* { **local** | **engineid** *engineid-string* | **remote** { *ipv4-address* | **ipv6** *ipv6-address* } }

Default

No SNMPv3 users exist.

Views

System view

Predefined user roles

network-admin

Parameters

user-name: Specifies an SNMPv3 username, a case-sensitive string of 1 to 32 characters.

group-name: Specifies an SNMPv3 group name, a case-sensitive string of 1 to 32 characters. The group can be one that has been created or not. The user takes effect only after you create the group.

user-role *role-name*: Specifies a user role name, a case-sensitive string of 1 to 63 characters.

remote { *ipv4-address* | **ipv6** *ipv6-address* }: Specifies a target host by its IPv4 or IPv6 address, typically the NMS, to receive the notifications. To send SNMPv3 notifications to a target host, you need to specify this option and use the **snmp-agent remote** command to bind the IPv4 or IPv6 address to the remote engine ID.

cipher: Specifies an authentication key and an encryption key in encrypted form. The keys will be converted to a digest in encrypted form and stored in the device.

simple: Specifies an authentication key and an encryption key in plaintext from. The keys will be converted to a digest in encrypted form and stored in the device.

authentication-mode: Specifies an authentication algorithm. If you do not specify the keyword, the system does not perform authentication. For more information about authentication algorithms, see IPSec configuration in *Security Configuration Guide*.

- **md5**: Specifies the HMAC-MD5 authentication algorithm.
- **sha**: Specifies the HMAC-SHA1 authentication algorithm.

auth-password: Specifies an authentication key. This argument is case sensitive.

- The plaintext form of the key in non-FIPS mode is a string of 1 to 64 characters. The plaintext form of the key in FIPS mode is a string of 15 to 64 characters, which must contain numbers, uppercase letters, lowercase letters, and special characters.
- The encrypted form of the key can be calculated by using the **snmp-agent calculate-password** command.

privacy-mode: Specifies an encryption algorithm. If you do not specify this keyword, the system does not perform encryption.

- **3des**: Specifies the 3DES encryption algorithm that uses a 168-bit key.
- **aes128**: Specifies the AES encryption algorithm that uses a 128-bit key.
- **aes192**: Specifies the AES encryption algorithm that uses a 192-bit key.
- **aes256**: Specifies the AES encryption algorithm that uses a 256-bit key.
- **des56**: Specifies the DES encryption algorithm that uses a 56-bit key.

priv-password: Specifies an encryption key. This argument is case sensitive.

- The plaintext form of the key in non-FIPS mode is a string of 1 to 64 characters. The plaintext form of the key in FIPS mode is a string of 15 to 64 characters, which must contain numbers, uppercase letters, lowercase letters, and special characters.
- The encrypted form of the key can be calculated by using the **snmp-agent calculate-password** command.

acl: Specifies a basic or advanced IPv4 ACL for the user.

ipv4-acl-number: Specifies a basic or advanced IPv4 ACL by its number. The basic IPv4 ACL number is in the range of 2000 to 2999. The advanced IPv4 ACL number is in the range of 3000 to 3999.

name *ipv4-acl-name*: Specifies a basic or advanced IPv4 ACL by its name, a case-insensitive string of 1 to 63 characters.

acl ipv6: Specifies a basic or advanced IPv6 ACL for the user.

ipv6-acl-number: Specifies a basic or advanced IPv6 ACL by its number. The basic IPv6 ACL number is in the range of 2000 to 2999. The advanced IPv6 ACL number is in the range of 3000 to 3999.

name *ipv6-acl-name*: Specifies a basic or advanced IPv6 ACL by its name, a case-insensitive string of 1 to 63 characters.

local: Specifies the local SNMP engine. By default, an SNMPv3 user is associated with the local SNMP engine.

engineid *engineid-string*: Specifies an SNMP engine ID. The *engineid-string* argument is an even number of hexadecimal characters. All-zero and all-F strings are invalid. The even number is in the range of 10 to 64. If you change the local engine ID, the existing SNMPv3 users and keys become invalid. To delete an invalid username, specify the engine ID associated with the username in the **undo snmp-agent usm-user v3** command.

Usage guidelines

Only users with the network-admin or level-15 user role can execute this command. Users with other user roles cannot execute this command even if these roles are granted access to commands of the SNMP feature or this command.

You can use either of the following modes to control SNMPv3 user access to MIB objects.

- **VACM**—Controls user access to MIB objects by assigning the user to an SNMP group. To make sure the user takes effect, make sure the group has been created. An SNMP group contains one or multiple users and specifies the MIB views and security model for the users. The authentication and encryption algorithms for each user are specified when they are created.
- **RBAC**—Controls user access to MIB objects by assigning user roles to the user. A user role specifies the MIB objects accessible to the user and the operations that the user can perform on the objects. After you create a user in RBAC mode, you can use the **snmp-agent usm-user v3 user-role** command to assign more user roles to the user. You can assign a maximum of 64 user roles to a user.

RBAC mode controls access on a per MIB object basis, and VACM mode controls access on a MIB view basis. As a best practice to enhance MIB security, use RBAC mode.

You can execute the **snmp-agent usm-user v3** command multiple times to create different SNMPv3 users in VACM mode. If you do not change the username each time, the most recent configuration takes effect.

You can execute the **snmp-agent usm-user v3** command in RBAC mode multiple times to assign different user roles to an SNMPv3 user. The following restrictions and guidelines apply:

- If you specify only user roles but do not change any other settings each time, the **snmp-agent usm-user v3** command assigns different user roles to the user. Other settings remain unchanged.
- If you specify user roles and also change other settings each time, the **snmp-agent usm-user v3** command assigns different user roles to the user. The most recent configuration for other settings takes effect.

You can specify an ACL for the user and group, respectively, to filter illegitimate NMSs from accessing the agent. Only the NMSs permitted by the ACLs for both the user and group can access the SNMP agent. The following rules apply to the ACLs for the user and group:

- If you do not specify an ACL, the specified ACL does not exist, or the specified ACL does not have any rules, all NMSs that use the username can access the SNMP agent.
- If you have specified an ACL and the ACL has rules, only the NMSs permitted by the ACL can access the agent.

For more information about ACL, see *ACL and QoS Configuration Guide*.

Examples

In VACM mode:

Add user **testUser** to SNMPv3 group **testGroup**, and enable authentication for the group. Specify authentication algorithm **HMAC-SHA1** and plaintext-form authentication key **123456TESTplat&!** for the user.

```
<Sysname> system-view
[Sysname] snmp-agent group v3 testGroup authentication
[Sysname] snmp-agent usm-user v3 testUser testGroup simple authentication-mode sha
123456TESTplat&!
```

For an NMS to access the MIB objects in the default view **ViewDefault**, make sure the following configurations on the NMS are the same as the SNMP agent:

- SNMPv3 username.
- SNMP protocol version.
- Authentication algorithm and key.

Add user **testUser** to SNMPv3 group **testGroup**, and enable authentication and encryption for the group. Specify authentication algorithm **HMAC-SHA1**, encryption algorithm **AES**, plaintext-form authentication key **123456TESTauth&!**, and plaintext-form encryption key **123456TESTencr&!** for the user.

```
<Sysname> system-view
[Sysname] snmp-agent group v3 testGroup privacy
[Sysname] snmp-agent usm-user v3 testUser testGroup simple authentication-mode sha
123456TESTauth&! privacy-mode aes128 123456TESTencr&!
```

For an NMS to access the MIB objects in the default view **ViewDefault**, make sure the following configurations on the NMS are the same as the SNMP agent:

- SNMPv3 username.
- SNMP protocol version.
- Authentication algorithm.
- Privacy algorithm.
- Plaintext authentication and encryption keys.

Add user **remoteUser** for the SNMP remote engine at 10.1.1.1 to SNMPv3 group **testGroup**, and enable authentication and encryption for the group. Specify authentication algorithm **HMAC-SHA1**, encryption algorithm **AES**, plaintext-form authentication key **123456TESTauth&!**, and plaintext-form encryption key **123456TESTencr&!** for the user.

```
<Sysname> system-view
[Sysname] snmp-agent remote 10.1.1.1 engineid 123456789A
[Sysname] snmp-agent group v3 testGroup privacy
[Sysname] snmp-agent usm-user v3 remoteUser testGroup remote 10.1.1.1 simple
authentication-mode sha 123456TESTauth&! privacy-mode aes128 123456TESTencr&!
```

In RBAC mode:

Create SNMPv3 user **testUser** with user role **network-operator** and enable authentication for the user. Specify authentication algorithm **HMAC-SHA1** and plaintext-form authentication key **123456TESTplat&!** for the user.

```
<Sysname> system-view
[Sysname] snmp-agent usm-user v3 testUser user-role network-operator simple
authentication-mode sha 123456TESTplat&!
```

For an NMS to have read-only access to all MIB objects, make sure the following configurations on the NMS are the same as the SNMP agent:

- SNMPv3 username.

- SNMP protocol version.
- Authentication algorithm and key.

Related commands

display snmp-agent usm-user

snmp-agent calculate-password

snmp-agent group

snmp-agent remote

snmp-agent usm-user v3 user-role

snmp-agent usm-user v3 user-role

Use **snmp-agent usm-user v3 user-role** to assign a user role to an SNMPv3 user created in RBAC mode.

Use **undo snmp-agent usm-user user-role** to remove a user role.

Syntax

snmp-agent usm-user v3 *user-name* **user-role** *role-name*

undo snmp-agent usm-user v3 *user-name* **user-role** *role-name*

Default

An SNMPv3 user has the user role assigned to it at its creation.

Views

System view

Predefined user roles

network-admin

Parameters

user-name: Specifies an SNMPv3 username, a case-sensitive string of 1 to 32 characters.

user-role *role-name*: Specifies a user role name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

You can assign a maximum of 64 user roles to an SNMPv3 user.

An SNMPv3 user must have a minimum of one user role.

Examples

Assign the user role **network-admin** to the SNMPv3 user **testUser**.

```
<Sysname> system-view
[Sysname] snmp-agent usm-user v3 testUser user-role network-admin
```

Related commands

snmp-agent usm-user v3

Contents

RMON commands

display rmon alarm

Use **display rmon alarm** to display information about RMON alarm entries.

Syntax

display rmon alarm [*entry-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

entry-number: Specifies an alarm entry by its index in the range of 1 to 65535. If you do not specify an entry, the command displays all RMON alarm entries.

Examples

Display information about all RMON alarm entries.

```
<Sysname> display rmon alarm
AlarmEntry 1 owned by user1 is VALID.
  Sample type                    : absolute
  Sampled variable               : 1.3.6.1.2.1.16.1.1.1.4.1<etherStatsOctets.1>
  Sampling interval (in seconds) : 10
  Rising threshold               : 50(associated with event 1)
  Falling threshold              : 5(associated with event 2)
  Alarm sent upon entry startup  : risingOrFallingAlarm
  Latest value                   : 0
```

Table 1 Command output

Field	Description

AlarmEntry *entry-number* owned by *owner* is *status*.	Alarm entry owner and status:
	• *entry-number*—Alarm entry index.
	• *owner*—Entry owner.
	• *status*—Entry status:
	  ○ **VALID**—The entry is valid.
	  ○ **UNDERCREATION**—The entry is invalid.
	The *status* field is not configurable at the CLI. All alarm entries created from the CLI are valid by default.
	The **display rmon alarm** command can display invalid entries, but the **display current-configuration** and **display this** commands do not display their settings.

Sample type	Sample type: • absolute. • delta.

Field	Description
Sampled variable	Monitored variable.
Sampling interval	Interval (in seconds) at which data is sampled.
Rising threshold	Alarm rising threshold.
associated with event	Event index associated with the alarm..
Falling threshold	Alarm falling threshold.
Alarm sent upon entry startup	Alarm that can be generated at the first sampling: • **risingAlarm**. • **fallingAlarm**. • **risingOrFallingAlarm**. The default is **risingOrFallingAlarm**.
Latest value	Most recent sampled value.

Related commands

rmon alarm

display rmon event

Use **display rmon event** to display information about RMON event entries.

Syntax

display rmon event [*entry-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

entry-number: Specifies an event entry by its index in the range of 1 to 65535. If you do not specify an entry, the command displays all event entries.

Usage guidelines

An event entry includes the following information:

- Event index.
- Event owner.
- Event description.
- Action triggered by the event (such as logging the event or sending an SNMP notification).
- Last time when the event occurred (seconds that elapsed since the system startup).

Examples

Display information about all RMON event entries.

```
<Sysname> display rmon event
EventEntry 1 owned by user1 is VALID.
  Description: N/A
```

```
Community: Security
Take the action log-trap when triggered, last triggered at 0days 00h:02m:27s uptime.
```

Table 2 Command output

Field	Description

EventEntry *entry-number* owned by *owner* is *status*.	Event entry owner and status:
	• *entry-number*—Event entry index.
	• *owner*—Entry owner.
	• *status*—Entry status:
	  ○ **VALID**—The entry is valid.
	  ○ **UNDERCREATION**—The entry is invalid.
	The *status* field is not configurable at the CLI. All alarm entries created from the CLI are valid by default.
	The **display rmon event** command can display invalid entries, but the **display current-configuration** and **display this** commands do not display their settings.

Description	Event description.
Community	SNMP community name for the RMON event.
Take the action *action* when triggered	Actions that the system takes when the event is triggered: • **none**—Takes no action. • **log**—Logs the event. • **trap**—Sends an SNMP notification. • **log-trap**—Logs the event and sends an SNMP notification.
last triggered at *time* uptime	Last time when the event occurred, which is represented as the amount of time that elapsed since the system startup.

Related commands

rmon event

display rmon eventlog

Use **display rmon eventlog** to display information about event log entries.

Syntax

display rmon eventlog [*entry-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

entry-number: Specifies an event entry by its index in the range of 1 to 65535. If you do not specify an entry, the command displays log entries for all event entries.

Usage guidelines

If the log action is specified for an event, the system adds a record in the event log table each time the event occurs. Each record contains the log entry index, time when the event was logged (the amount of time that elapsed since system startup), and event description.

The system can maintain a maximum of 10 records for an event. The most recent record replaces the oldest record if the number of records reaches 10.

Examples

Display the RMON log for event entry **99**.

```
<Sysname> display rmon eventlog 99
EventEntry 99 owned by ww is VALID.
  LogEntry 99.1 created at 50days 08h:54m:44s uptime.
  Description: The 1.3.6.1.2.1.16.1.1.1.4.5 defined in alarmEntry 77,
     uprise 16760000 with alarm value 16776314. Alarm sample type is absolute.
  LogEntry 99.2 created at 50days 09h:11m:13s uptime.
  Description: The 1.3.6.1.2.1.16.1.1.1.4.5 defined in alarmEntry 77,
     less than(or =) 20000000 with alarm value 16951648. Alarm sample type is absolute.
  LogEntry 99.3 created at 50days 09h:18m:43s uptime.
  Description: The alarm formula defined in prialarmEntry 777,
     less than(or =) 15000000 with alarm value 14026493. Alarm sample type is absolute.
  LogEntry 99.4 created at 50days 09h:23m:28s uptime.
  Description: The alarm formula defined in prialarmEntry 777,
     uprise 17000000 with alarm value 17077846. Alarm sample type is absolute.
```

This example shows that the event log table has four records for event 99:

- Two records were created when event 99 was triggered by alarm entry 77.
- Two records were created when event 99 was triggered by private alarm entry 777.

Table 3 Command output

Field	Description

EventEntry *entry-number* owned by *owner* is *status*.	Event log entry owner and status:
	• *entry-number*—Event log entry index, which is the same as the event entry index for which this log entry is generated.
	• *owner*—Entry owner.
	• *status*—Entry status:
	  ○ **VALID**—The entry is valid (default value).
	  ○ **UNDERCREATION**—The entry is invalid.
	The *status* field is not configurable at the CLI. All event log entries are valid by default.
	The **display rmon eventlog** command can display invalid entries, but the **display current-configuration** and **display this** commands do not display their settings.

LogEntry *entry-number* created at *created-time* uptime.	Time when an event record was created: • *entry-number*—Event record index, represented as logEventIndex.logIndex, where logEventIndex and logIndex are MIB objects. A record index uniquely identifies a record among all records for the event. • *created-time*—Time when the event entry was created.
Description	Record description.

Related commands

rmon event

display rmon history

Use **display rmon history** to display RMON history control entries and history samples of Ethernet statistics for Ethernet interfaces.

Syntax

display rmon history [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type i*nterface-number*: Specifies an interface by its type and number. If you do not specify an interface, the command displays history samples for all interfaces that have an RMON history control entry.

Usage guidelines

RMON uses the etherHistoryTable object to store the history samples of Ethernet statistics for Ethernet interfaces.

To collect history samples for an Ethernet interface, you must first create a history control entry on the interface.

To configure the number of history samples that can be displayed and the history sampling interval, use the **rmon history** command.

Examples

Display the RMON history control entry and history samples for GigabitEthernet 1/0/1.

```
<Sysname> display rmon history gigabitethernet 1/0/1
HistoryControlEntry 6 owned by user1 is VALID.
  Sampled interface     : GigabitEthernet1/0/1<ifIndex.117>
  Sampling interval     : 8(sec) with 3 buckets max
  Sampling record 1 :
    dropevents        : 0         , octets               : 5869
    packets           : 54        , broadcast packets    : 9
    multicast packets : 23        , CRC alignment errors : 0
    undersize packets : 0         , oversize packets     : 0
    fragments         : 0         , jabbers              : 0
    collisions        : 0         , utilization          : 0
```

Table 4 Command output

Field	Description

HistoryControlEntry *entry-number* owned by *owner* is *status*.	Status and owner of the history control entry:
	• *entry-number*—History control entry index.
	• *owner*—Entry owner.
	• *status*—Entry status:
	  ○ **VALID**—The entry is valid.
	  ○ **UNDERCREATION**—The entry is invalid.
	The *status* field is not configurable at the CLI. All history control entries created from the CLI are valid by default.
	The **`display rmon history`** command can display invalid entries, but the **`display current-configuration`** and **`display this`** commands do not display their settings.

Sampled Interface	Sampled interface.
Sampling interval	Sampling interval in seconds.
buckets max	Maximum number of samples that can be saved for the history control entry. If the expected bucket size specified with the **`rmon history`** command exceeds the available history table size, RMON sets the bucket size as closely to the expected bucket size as possible. If the bucket has been full, RMON overwrites the oldest sample with the new sample.
Sampling record	History sample index.
dropevents	Total number of events in which packets were dropped during the sampling interval. **NOTE:** This statistic is the number of times that a drop condition occurred. It is not necessarily the total number of dropped packets.
octets	Total number of octets received during the sampling interval.
packets	Total number of packets (including bad packets) received during the sampling interval.
broadcast packets	Number of broadcast packets received during the sampling interval.
multicast packets	Number of multicast packets received during the sampling interval.
CRC alignment errors	Number of packets received with CRC alignment errors during the sampling interval.
undersize packets	Number of undersize packets received during the sampling interval. Undersize packets are shorter than 64 octets (excluding framing bits but including FCS octets).
oversize packets	Number of oversize packets received during the sampling interval. An oversize packet is a packet that exceeds the maximum frame length (excluding framing bits but including FCS octets) specified by the **jumboframe enable** command. For more information about the **jumboframe enable** command, see Ethernet interfaces in *Interface Command Reference*.
fragments	Number of undersize packets with CRC errors received during the sampling interval.
jabbers	Number of oversize packets with CRC errors received during the sampling interval.
collisions	Number of colliding packets received during the sampling interval.

Field	Description
utilization	Bandwidth utilization (in hundreds of a percent) during the sampling period.

Related commands

rmon history

display rmon prialarm

Use **display rmon prialarm** to display information about RMON private alarm entries.

Syntax

display rmon prialarm [*entry-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

entry-number: Specifies an alarm entry index in the range of 1 to 65535. If you do not specify an entry, the command displays all private alarm entries.

Examples

Display information about all RMON private alarm entries.

```
<Sysname> display rmon prialarm
PrialarmEntry 1 owned by user1 is VALID.
  Sample type                    : absolute
  Variable formula          : (.1.3.6.1.2.1.16.1.1.1.6.1*100/.1.3.6.1.2.1.16.1.1.1.5.1)
  Description                    : ifUtilization.GigabitEthernet1/0/1
  Sampling interval (in seconds) : 10
  Rising threshold               : 80(associated with event 1)
  Falling threshold              : 5(associated with event 2)
  Alarm sent upon entry startup  : risingOrFallingAlarm
  Entry lifetime                 : forever
  Latest value                   : 85
```

Table 5 Command output

Field	Description

PrialarmEntry *entry-number* owned by *owner* is *status*.	Alarm entry owner and status:
	• *entry-number*—Alarm entry index.
	• *owner*—Entry owner.
	• *status*—Entry status:
	  ○ **VALID**—The entry is valid.
	  ○ **UNDERCREATION**—The entry is invalid.
	The *status* field is not configurable at the CLI. All alarm entries created from the CLI are valid by default.
	The **display rmon prialarm** command can display invalid entries, but the **display current-configuration** and **display this** commands do not display their settings.

Sample type	Sample type: • absolute. • delta.
Variable formula	Variable formula.
Description	Description of the alarm.
Sampling interval	Interval (in seconds) at which data is sampled.
Rising threshold	Alarm rising threshold.
Falling threshold	Alarm falling threshold.
associated with event	Event index associated with the alarm..
Alarm sent upon entry startup	Alarm that can be generated at the first sampling: • **risingAlarm**. • **fallingAlarm**. • **risingOrFallingAlarm**. The default is **risingOrFallingAlarm**.
Entry lifetime	Lifetime of the entry. • If the lifetime is set to **forever**, the entry never expires. • If the lifetime is set to an amount of time, the entry is removed when the timer expires.
Latest value	Most recent sampled value.

Related commands

rmon prialarm

display rmon statistics

Use **display rmon statistics** to display RMON statistics.

Syntax

display rmon statistics [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, the command displays RMON statistics for all interfaces.

Usage guidelines

This command displays the cumulative interface statistics for the period from the time the statistics entry was created to the time the command was executed. The statistics are cleared when the device reboots.

Examples

Display RMON statistics for GigabitEthernet 1/0/1.

```
<Sysname> display rmon statistics gigabitethernet 1/0/1
EtherStatsEntry 1 owned by user1 is VALID.
  Interface : GigabitEthernet1/0/1<ifIndex.3>
  etherStatsOctets         : 43393306  , etherStatsPkts          : 619825
  etherStatsBroadcastPkts  : 503581    , etherStatsMulticastPkts : 44013
  etherStatsUndersizePkts  : 0         , etherStatsOversizePkts  : 0
  etherStatsFragments      : 0         , etherStatsJabbers       : 0
  etherStatsCRCAlignErrors : 0         , etherStatsCollisions    : 0
  etherStatsDropEvents (insufficient resources): 0
  Incoming packets by size:
  64     : 0         ,  65-127  : 0         ,  128-255  : 0
  256-511: 0         ,  512-1023: 0         ,  1024-1518: 0
```

Table 6 Command output

Field	Description

EtherStatsEntry *entry-number* owned by *owner* is *status*.	Statistics entry owner and status:
	• *entry-number*—Statistics entry index.
	• *owner*—Entry owner.
	• *status*—Entry status:
	  ○ **VALID**—The entry is valid.
	  ○ **UNDERCREATION**—The entry is invalid.
	The *status* field is not configurable at the CLI. All alarm entries created from the CLI are valid by default.
	The **display rmon statistics** command can display invalid entries, but the **display current-configuration** and **display this** commands do not display their settings.

Interface	Interface on which statistics are gathered.
etherStatsOctets	Total number of octets received on the interface.
etherStatsPkts	Total number of packets received on the interface.
etherStatsBroadcastPkts	Total number of broadcast packets received on the interface.
etherStatsMulticastPkts	Total number of multicast packets received on the interface.
etherStatsUndersizePkts	Total number of undersize packets received on the interface.

Field	Description
etherStatsOversizePkts	Total number of oversize packets received on the interface. An oversize packet is a packet that exceeds the maximum frame length (excluding framing bits but including FCS octets) specified by the **jumboframe enable** command. For more information about the **jumboframe enable** command, see Ethernet interfaces in *Interface Command Reference*.
etherStatsFragments	Total number of undersize packets received with CRC errors on the interface.
etherStatsJabbers	Total number of oversize packets received with CRC errors on the interface.
etherStatsCRCAlignErrors	Total number of packets received with CRC errors on the interface.
etherStatsCollisions	Total number of colliding packets received on the interface.
etherStatsDropEvents	Total number of events in which packets were dropped. **NOTE:** This statistic is the number of times that a drop condition occurred. It is not necessarily the total number of dropped packets.
Incoming packets by size:	Incoming-packet statistics by packet length: • **64**—Number of packets with a length equal to 64 bytes. • **65-127**—Number of 65- to 127-byte packets. • **128-255**—Number of 128- to 255-byte packets. • **256-511**—Number of 256- to 511-byte packets. • **512-1023**—Number of 512- to 1023-byte packets. • **1024-1518**—Number of 1024- to 1518-byte packets.

Related commands

rmon statistics

rmon alarm

Use **rmon alarm** to create an RMON alarm entry.

Use **undo rmon alarm** to remove an RMON alarm entry.

Syntax

rmon alarm *entry-number alarm-variable sampling-interval* { **absolute** | **delta** } [**startup-alarm** { **falling** | **rising** | **rising-falling** }] **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* [**owner** *text*]

undo rmon alarm *entry-number*

Default

No RMON alarm entries exist.

Views

System view

Predefined user roles

network-admin

Parameters

entry-number: Specifies an alarm entry index in the range of 1 to 65535.

alarm-variable: Specifies an alarm variable, a string of 1 to 255 characters. You can only specify variables that can be parsed as an ASN.1 INTEGER value (INTEGER, INTEGER32, Unsigned32, Counter32, Counter64, Gauge, or TimeTicks) for the *alarm-variable* argument. The alarm variables must use one of the formats in Table 7.

Table 7 Alarm variable formats

Format	Examples
Dotted OID format: *entry.integer.instance*	1.3.6.1.2.1.2.1.10.1
Object name.instance	etherStatsOctets.1 etherStatsPkts.1 etherStatsBroadcastPkts.1 ifInOctets.1 ifInUcastPkts.1 ifInNUcastPkts.1

sampling-interval: Sets the sampling interval in the range of 5 to 65535 seconds.

absolute: Specifies absolute sampling. RMON compares the value of the variable with the rising and falling thresholds.

delta: Specifies delta sampling. RMON subtracts the value of the variable at the previous sample from the current sampled value, and then compares the difference with the rising and falling thresholds.

startup-alarm: Specifies alarms that can be generated at the first sampling when a rising or falling threshold is reached or exceeded. By default, a **rising-falling** alarm is generated.

rising: Generates a rising alarm.

falling: Generates a falling alarm.

rising-falling: Generates a rising or falling alarm.

rising-threshold *threshold-value1 event-entry1*: Sets the rising threshold. The *threshold-value1* argument represents the rising threshold in the range of –2147483648 to 2147483647. The *event-entry1* argument represents the index of the event that is triggered when the rising threshold is crossed. The value range for the *event-entry1* argument is 0 to 65535. If 0 is specified, the alarm does not trigger any event.

falling-threshold *threshold-value2 event-entry2*: Sets the falling threshold. The *threshold-value2* argument represents the falling threshold in the range of –2147483648 to 2147483647. The *event-entry2* argument represents the index of the event that is triggered when the falling threshold is crossed. The value range for the *event-entry2* argument is 0 to 65535. If 0 is specified, the alarm does not trigger any event.

owner *text*: Specifies the entry owner, a case-sensitive string of 1 to 127 characters.

Usage guidelines

You can create a maximum of 60 RMON alarm entries.

Each alarm entry must have a unique alarm variable, sampling interval, sample type, rising threshold, or falling threshold. You cannot create an alarm entry if all these parameters for the entry are the same as an existing entry.

To trigger the event associated with an alarm condition, you must create the event with the **rmon event** command.

RMON samples the monitored alarm variable at the specified sampling interval, compares the sampled value with the predefined thresholds, and performs one of the following operations:

- Triggers the event associated with the rising alarm if the sampled value is equal to or greater than the rising threshold.
- Triggers the event associated with the falling alarm if the sampled value is equal to or less than the falling threshold.

Examples

Create an alarm entry to perform absolute sampling on the number of octets received on GigabitEthernet 1/0/1 (object instance 1.3.6.1.2.1.16.1.1.1.4.1) at 10-seconds intervals. If the sampled value reaches or exceeds 5000, log the rising alarm event. If the sampled value is equal to or less than 5, take no actions.

```
<Sysname> system-view
[Sysname] rmon event 1 log
[Sysname] rmon event 2 none
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon statistics 1
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] rmon alarm 1 1.3.6.1.2.1.16.1.1.1.4.1 10 absolute rising-threshold 5000 1
falling-threshold 5 2 owner user1
```

In this example, you can replace 1.3.6.1.2.1.16.1.1.1.4.1 with etherStatsOctets.1, where 1 is the statistics entry index for the interface. If you execute the **rmon statistics 5** command, you can use etherStatsOctets.5 to replace 1.3.6.1.2.1.16.1.1.1.4.5.

Related commands

display rmon alarm

rmon event

rmon event

Use **rmon event** to create an RMON event entry.

Use **undo rmon event** to remove an RMON event entry.

Syntax

rmon event *entry-number* [**description** *string*] { **log** | **log-trap** *security-string* | **none** | **trap** *security-string* } [**owner** *text*]

undo rmon event *entry-number*

Default

No RMON event entries exist.

Views

System view

Predefined user roles

network-admin

Parameters

entry-number: Specifies an event entry index in the range of 1 to 65535.

description *string*: Configures an event description, a case-sensitive string of 1 to 127 characters.

log: Logs the event .

log-trap: Logs the event and sends an SNMP notification.

security-string: Specifies the SNMP community name carried in the SNMP notifications. The *security-string* argument is a case-sensitive string of 1 to 127 characters and is determined by the SNMP configuration. This argument is supported but does not take effect in the current software version.

none: Performs no action.

trap: Sends an SNMP notification.

owner *text*: Specifies the entry owner, a case-sensitive string of 1 to 127 characters.

NOTE:

The SNMP community name setting for the *security-string* argument does not take effect even though you can configure it with the command. Instead, the system uses the settings you configure with SNMP when it sends RMON SNMP notifications. For more information about SNMP notifications, see *Network Management and Monitoring Configuration Guide*.

Usage guidelines

You can create a maximum of 60 event entries.

You can associate an event entry with a standard or private alarm entry to specify the action to take when an alarm condition occurs. Depending on your configuration, the system logs the event, sends an SNMP notification, does both, or does neither.

You can associate an event with multiple alarm entries.

Examples

Create an RMON log event entry. Specify its index as **10** and the entry owner as **user1**.

```
<Sysname> system-view
[Sysname] rmon event 10 log owner user1
```

Related commands

display rmon event

rmon alarm

rmon prialarm

rmon history

Use **rmon history** to create an RMON history control entry.

Use **undo rmon history** to remove an RMON history control entry.

Syntax

rmon history *entry-number* **buckets** *number* **interval** *interval* [**owner** *text*]

undo rmon history *entry-number*

Default

No RMON history control entries exist.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

entry-number: Specifies a history control entry index in the range of 1 to 65535.

buckets *number*: Specifies the expected maximum number of samples to be retained for the entry, in the range of 1 to 65535. RMON can retain a maximum of 50 samples for each history control entry. If the expected bucket size exceeds the available history table size, RMON sets the bucket size as closely to the expected bucket size as is possible. However, the granted bucket size will not exceed 50. For example, the bucket size for a history control entry will be 30 if the expected bucket size is set to 55, but the available bucket size is only 30.

interval *interval*: Specifies the sampling interval in the range of 5 to 3600 seconds.

owner *text*: Specifies the entry owner, a case-sensitive string of 1 to 127 characters.

Usage guidelines

The system supports a maximum of 100 history control entries.

If an Ethernet interface has a history control entry, RMON periodically samples packet statistics on the interface and stores the samples to the history table. When the bucket size for the history control entry is reached, RMON overwrites the oldest sample with the most recent sample.

You can create multiple RMON history control entries for an Ethernet interface.

Examples

Create RMON history control entry 1 for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon history 1 buckets 10 interval 5 owner user1
```

Related commands

display rmon history

rmon prialarm

Use **rmon** *prialarm* to create an RMON private alarm entry.

Use **undo rmon** *prialarm* to remove an RMON private alarm entry.

Syntax

rmon prialarm *entry-number prialarm-formula prialarm-des sampling-interval* { **absolute** | **delta** } [**startup-alarm** { **falling** | **rising** | **rising-falling** }] **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* **entrytype** { **forever** | **cycle** *cycle-period* } [**owner** *text*]

undo rmon prialarm *entry-number*

Default

No RMON private alarm entries exist.

Views

System view

Predefined user roles

network-admin

Parameters

entry-number: Specifies a private alarm entry index in the range of 1 to 65535.

prialarm-formula: Configures a private alarm variable formula, a string of 1 to 255 characters. The variables in the formula must be represented in OID format that starts with a dot (.), for example, (.1.3.6.1.2.1.2.1.10.1)*8. You can configure a formula to perform the basic math operations of addition, subtraction, multiplication, and division on these variables. To get a correct calculation result, make sure the following conditions are met:

- The values of the variables in the formula are positive integers.
- The result of each calculating step is in the value range for long integers.

prialarm-des: Configures an entry description, a case-sensitive string of 1 to 127 characters.

sampling-interval: Sets the sampling interval in the range of 10 to 65535 seconds.

absolute: Specifies absolute sampling. RMON compares the value of the variable with the rising and falling thresholds.

delta: Specifies delta sampling. RMON subtracts the value of the variable at the previous sample from the current sampled value, and then compares the difference with the rising and falling thresholds.

startup-alarm: Specifies alarms that can be generated at the first sampling when a rising or falling threshold is reached or exceeded. By default, a **rising-falling** alarm is generated.

rising: Generates a rising alarm.

falling: Generates a falling alarm.

rising-falling: Generates a rising or falling alarm.

rising-threshold *threshold-value1 event-entry1*: Sets the rising threshold. The *threshold-value1* argument represents the rising threshold in the range of –2147483648 to 2147483647. The *event-entry1* argument represents the index of the event that is triggered when the rising threshold is crossed. The value range for the *event-entry1* argument is 0 to 65535. If 0 is specified, the alarm does not trigger any event.

falling-threshold *threshold-value2 event-entry2*: Sets the falling threshold. The *threshold-value2* argument represents the falling threshold in the range of –2147483648 to 2147483647. The *event-entry2* argument represents the index of the event that is triggered when the falling threshold is crossed. The value range for the *event-entry2* argument is 0 to 65535. If 0 is specified, the alarm does not trigger any event.

forever: Configures the entry as a permanent entry. RMON retains a permanent private alarm entry until it is manually deleted.

cycle *cycle-period*: Sets the lifetime of the entry, in the range of 0 to 4294967 seconds. RMON deletes the entry when its lifetime expires.

owner *text*: Specifies the entry owner, a case-sensitive string of 1 to 127 characters.

Usage guidelines

You can create a maximum of 50 private alarm entries.

Each alarm entry must have a unique alarm variable, sampling interval, sample type, rising threshold, or falling threshold. You cannot create an alarm entry if all these parameters for the entry are the same as an existing entry.

To trigger the event associated with an alarm condition, you must create the event with the **rmon event** command.

The RMON agent samples variables and takes an alarm action based on a private alarm entry as follows:

1. Periodically samples the variables specified in the private alarm formula.
2. Processes the sampled values with the formula.
3. Compares the calculation result with the predefined thresholds, and then takes one of the following actions:
   - Triggers the event associated with the rising alarm event if the result is equal to or greater than the rising threshold.
   - Triggers the event associated with the falling alarm event if the result is equal to or less than the falling threshold.

Examples

Add a permanent private alarm entry to monitor the ratio of incoming broadcasts to the total number of incoming packets on GigabitEthernet 1/0/1. Log the rising alarm event when the ratio exceeds 80%, and take no actions when the ratio drops to 5%. The formula is (1.3.6.1.2.1.16.1.1.1.6.1*100/.1.3.6.1.2.1.16.1.1.1.5.1), where 1.3.6.1.2.1.16.1.1.1.6.1 is the OID of the object instance etherStatsBroadcastPkts.1, and 1.3.6.1.2.1.16.1.1.1.5.1 is the OID of the object instance etherStatsPkts.1.

```
<Sysname> system-view
[Sysname] rmon event 1 log
[Sysname] rmon event 2 none
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon statistics 1
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] rmon prialarm 1 (.1.3.6.1.2.1.16.1.1.1.6.1*100/.1.3.6.1.2.1.16.1.1.1.5.1)
BroadcastPktsRatioOfGE1/0/1 10 absolute rising-threshold 80 1 falling-threshold 5 2
entrytype forever owner user1
```

The last number in the OID forms of variables must be the same as the statistics entry index for the interface. For example, if you execute the **rmon statistics 5** command, you must replace 1.3.6.1.2.1.16.1.1.1.6.1 and 1.3.6.1.2.1.16.1.1.1.5.1 with 1.3.6.1.2.1.16.1.1.1.6.5 and 1.3.6.1.2.1.16.1.1.1.5.5, respectively.

Related commands

display rmon prialarm

rmon event

rmon statistics

Use **rmon statistics** to create an RMON statistics entry.

Use **undo rmon statistics** to remove an RMON statistics entry.

Syntax

rmon statistics *entry-number* [**owner** *text*]

undo rmon statistics *entry-number*

Default

No RMON statistics entries exist.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

entry-number: Specifies a statistics entry index in the range of 1 to 65535.

owner *text*: Specifies the entry owner, a case-sensitive string of 1 to 127 characters.

Usage guidelines

Each RMON statistics entry provides a set of cumulative traffic statistics collected up to the present time for an interface. Statistics include number of collisions, CRC alignment errors, number of undersize or oversize packets, number of broadcasts, number of multicasts, number of bytes received, and number of packets received. The statistics are cleared at a reboot.

To display the RMON statistics table, use the **display rmon statistics** command.

The index of an RMON statistics entry must be globally unique. If the index has been used by another interface, the creation operation fails.

You can create only one RMON statistics entry for an Ethernet interface.

Examples

Create an RMON statistics entry for GigabitEthernet 1/0/1. The index is 20 and the owner is **user1**.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon statistics 20 owner user1
```

Related commands

display rmon statistics

Contents

NETCONF commands

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

netconf capability specific-namespace

Use **netconf capability specific-namespace** to configure the device to use module-specific namespaces.

Use **undo netconf capability specific-namespace** to restore the default.

Syntax

netconf capability specific-namespace

undo netconf capability specific-namespace

Default

The device uses the common namespace.

Views

System view

Predefined user roles

network-admin

Usage guidelines

NETCONF supports both the common namespace and module-specific namespaces. The common namespace is incompatible with module-specific namespaces. To set up a NETCONF session, the device and the client must use the same type of namespaces. By default, the common namespace is used. If the client does not support the common namespace, use this command to configure the device to use module-specific namespaces.

For this command to take effect, you must reestablish the NETCONF session.

Examples

Configure the device to use module-specific namespaces.

```
<Sysname> system-view
[Sysname] netconf capability specific-namespace
```

netconf idle-timeout

Use **netconf idle-timeout** to set the NETCONF session idle timeout time.

Use **undo netconf idle-timeout** to restore the default.

Syntax

netconf { **soap** | **agent** } **idle-timeout** *minute*

undo netconf { **soap** | **agent** } **idle-timeout**

Default

The NETCONF session idle timeout time is 10 minutes for NETCONF over SOAP over HTTP sessions and NETCONF over SOAP over HTTPS sessions.

The NETCONF session idle timeout time is 0 minutes for NETCONF over SSH sessions, NETCONF over Telnet sessions, and NETCONF over console sessions. The sessions never time out.

Views

System view

Predefined user roles

network-admin

Parameters

soap: Specifies the NETCONF over SOAP over HTTP sessions and NETCONF over SOAP over HTTPS sessions.

agent: Specifies the NETCONF over SSH sessions, NETCONF over Telnet sessions, and NETCONF over console sessions.

minute: Specifies the NETCONF session idle timeout time in minutes. The value range is as follows:

- 1 to 999 for NETCONF over SOAP over HTTP sessions and NETCONF over SOAP over HTTPS sessions.
- 0 to 999 for NETCONF over SSH sessions, NETCONF over Telnet sessions, and NETCONF over console sessions. To disable the timeout feature, set this argument to 0.

Usage guidelines

If no NETCONF packets are exchanged on a NETCONF session within the NETCONF session idle timeout time, the device tears down the session.

Examples

Set the NETCONF session idle timeout time to 20 minutes for NETCONF over SOAP over HTTP sessions and NETCONF over SOAP over HTTPS sessions.

```
<Sysname> system-view
[Sysname] netconf soap idle-timeout 20
```

netconf log

Use **netconf log** to enable NETCONF logging.

Use **undo netconf log** to remove the configuration for the specified NETCONF operation sources and NETCONF operations.

Syntax

netconf log source { **all** | { **agent** | **soap** | **web** } * } { **protocol-operation** { **all** | { **action** | **config** | **get** | **session** | **set** | **syntax** | **others** } * } | **row-operation** | **verbose** }

undo netconf log source { **all** | { **agent** | **soap** | **web** } * } { **protocol-operation** { **all** | { **action** | **config** | **get** | **session** | **set** | **syntax** | **others** } * } | **row-operation** | **verbose** }

Default

NETCONF logging is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

source: Specifies a NETCONF operation source that represents clients that use a protocol.

- **all**: Specifies NETCONF clients that use all protocols.
- **agent**: Specifies clients that use Telnet, SSH, NETCONF over console, or NETCONF over SSH.
- **soap**: Specifies clients that use SOAP over HTTP, or SOAP over HTTPS.
- **web**: Specifies clients that use Web.

protocol-operation: Logs requests and replies for specific types of NETCONF operations.

- **all**: Specifies all types of NETCONF operations.
- **action**: Specifies the <action> operation.
- **config**: Specifies the configuration-related NETCONF operations, including the <CLI>, <save>, <load>, <rollback>, <lock>, <unlock>, and <save-point> operations.
- **get**: Specifies the data retrieval-related NETCONF operations, including the <get>, <get-config>, <get-bulk>, <get-bulk-config>, and <get-sessions> operations.
- **session**: Specifies session-related NETCONF operations, including the <kill-session> and <close-session> operations, and capability exchanges by hello messages.
- **set**: Specifies all <edit-config> operations.
- **syntax**: Specifies the requests that include XML and schema errors.
- **others**: Specifies NETCONF operations except for those specified by keywords **action**, **config**, **get**, **set**, **session**, and **syntax**.

row-operation: Logs row operations for <action> and <edit-config> operations.

verbose: Logs detailed information about requests and replies for types of NETCONF operations, including packet contents of format-correct requests and error information about failed <edit-config> operations.

Usage guidelines

If you specify the **protocol-operation** keyword, the device logs each of the matching operation and the operation result. For example, if you perform a NETCONF operation to create VLANs 3 through 5, the device outputs the following log messages:

```
%Mar 21 17:11:34:479 2017 Sysname XMLSOAP/6/XML_REQUEST: test from 192.168.100.198,
session id 2,message-id 100, receive edit-config request.
%Mar 21 17:11:34:483 2017 Sysname XMLSOAP/6/EDIT-CONFIG: test from 192.168.100.198,
session id 2,message-id 100, execute success.
```

If you specify the **row-operation** keyword, the device logs each row operation and the operation result for an <action> or <edit-config> operation. For example, if you perform a NETCONF operation to create VLANs 3 through 5, the device outputs the following log messages:

```
%Mar 31 17:50:02:608 2017 Sysname XMLSOAP/6/EDIT-CONFIG: User (test, 192.168.100.20,
session ID 1), message ID=100, operation=create VLAN/VLANs (ID=3), result=Succeeded. No
attributes.
%Mar 31 17:50:02:609 2017 Sysname XMLSOAP/6/EDIT-CONFIG: User (test, 192.168.100.20,
session ID 1), message ID=100, operation=create VLAN/VLANs (ID=4), result=Succeeded. No
attributes.
%Mar 31 17:50:02:611 2017 Sysname XMLSOAP/6/EDIT-CONFIG: User (test, 192.168.100.20,
session ID 1), message ID=100, operation=create VLAN/VLANs (ID=5), result=Succeeded. No
attributes.
```

For NETCONF to correctly send the generated logs to the information center, you must also configure the information center. For information about information center configuration, see *Network Management and Monitoring Configuration Guide*.

Examples

Configure the device to log NETCONF edit-config information sourced from agent clients.

```
<Sysname> system-view
[Sysname] netconf log source agent protocol-operation set
```

netconf soap acl

Use **netconf soap acl** to apply an IPv4 ACL to control NETCONF over SOAP access.

Use **undo netconf soap acl** to restore the default.

Syntax

In non-FIPS mode:

netconf soap { **http** | **https** } **acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }

undo netconf soap { **http** | **https** } **acl**

In FIPS mode:

netconf soap https acl { *ipv4-acl-number* | **name** *ipv4-acl-name* }

undo netconf soap https acl

Default

No IPv4 ACL is applied to control NETCONF over SOAP access.

Views

System view

Predefined user roles

network-admin

Parameters

ipv4-acl-number: Specifies an IPv4 ACL by its number in the range of 2000 to 2999.

http: Applies an IPv4 ACL to control NETCONF over SOAP over HTTP access.

https: Applies an IPv4 ACL to control NETCONF over SOAP over HTTPS access.

name *ipv4-acl-name*: Specifies an IPv4 ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters. It must start with an English letter. To avoid confusion, it cannot be **all**.

Usage guidelines

To control NETCONF over SOAP access, specify an ACL that exists and has rules.

- If the specified ACL exists and has rules, only clients permitted by the ACL can establish NETCONF over SOAP sessions.
- If no ACL is applied or the applied ACL does not exist or does not have rules, all NETCONF clients can establish NETCONF over SOAP sessions.

If you execute the **netconf soap http acl** command multiple times, the most recent configuration takes effect. The same is true for the **netconf soap https acl** command.

Examples

Use IPv4 ACL 2001 to allow only NETCONF clients from subnet 10.10.0.0/16 to establish NETCONF over SOAP over HTTP sessions.

```
<Sysname> system-view
[Sysname] acl basic 2001
```

```
[Sysname-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] netconf soap http acl 2001
```

netconf soap domain

Use **netconf soap domain** to specify a mandatory authentication domain for NETCONF users.

Use **undo netconf soap domain** to restore the default.

Syntax

netconf soap domain *domain-name*

undo netconf soap domain

Default

No mandatory authentication domain is specified for NETCONF users.

Views

System view

Predefined user roles

network-admin

Parameters

domain-name: Specifies an ISP domain by its name, a case-insensitive string of 1 to 255 characters. For information about ISP domains, see *Security Configuration Guide*.

Usage guidelines

You can use either of the following methods to specify an authentication domain:

- Execute the **netconf soap domain** command to specify a mandatory authentication domain. After this command is executed, all NETCONF users are placed in the domain for authentication.
- Add an authentication domain to the <UserName> parameter of a SOAP request. The authentication domain takes effect only on the current request.

The authentication domain specified by using this command takes precedence over the authentication domain specified by the <UserName> parameter of a SOAP request.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify mandatory authentication domain **my-domain** for NETCONF users.

```
<Sysname> system-view
[Sysname] netconf soap domain my-domain
```

netconf soap dscp

Use **netconf soap dscp** to set the DSCP value for outgoing NETCONF over SOAP packets.

Use **undo netconf soap dscp** to restore the default.

Syntax

In non-FIPS mode:

netconf soap { **http** | **https** } **dscp** *dscp-value*

undo netconf soap { **http** | **https** } **dscp**

In FIPS mode:

netconf soap https dscp *dscp-value*

undo netconf soap https dscp

Default

The DSCP value is 0 for outgoing NETCONF over SOAP packets.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63. A larger DSCP value represents a higher priority.

http: Specifies NETCONF over SOAP over HTTP packets.

https: Specifies NETCONF over SOAP over HTTPS packets.

Usage guidelines

The DSCP value of an IP packet specifies the priority level of the packet and affects the transmission priority of the packet.

Examples

Set the DSCP value to 30 for outgoing NETCONF over SOAP over HTTP packets.

```
<Sysname> system-view
[Sysname] netconf soap http dscp 30
```

netconf soap enable

Use **netconf soap enable** to enable NETCONF over SOAP.

Use **undo netconf soap enable** to disable NETCONF over SOAP.

Syntax

In non-FIPS mode:

netconf soap { **http** | **https** } **enable**

undo netconf soap { **http** | **https** } **enable**

In FIPS mode:

netconf soap https enable

undo netconf soap https enable

Default

If the device starts up with the initial configuration, NETCONF over SOAP is disabled.

If the device starts up with the factory defaults, the enabling state of NETCONF over SOAP varies depending on the hardware platform and software version, as shown in Table 1.

Table 1 Factory defaults for NETCONF over SOAP

Feature	Factory default	Applicable software versions
NETCONF over SOAP over HTTPS	Disabled	All versions
NETCONF over SOAP over HTTP	Disabled	Versions earlier than Release 6348P01
	Enabled	Release 6348P01 or later

For more information about initial configuration, factory defaults, and startup configuration, see configuration file management in *Fundamentals Configuration Guide*.

Views

System view

Predefined user roles

network-admin

Parameters

`http`: Specifies NETCONF over SOAP over HTTP.

`https`: Specifies NETCONF over SOAP over HTTPS.

Usage guidelines

This command enables the device to resolve NETCONF messages that are encapsulated with SOAP in HTTP or HTTPS packets.

Examples

Enable NETCONF over SOAP over HTTP.

```
<Sysname> system-view
[Sysname] netconf soap http enable
```

netconf ssh server enable

Use **`netconf ssh server enable`** to enable NETCONF over SSH.

Use **`undo netconf ssh server enable`** to disable NETCONF over SSH.

Syntax

`netconf ssh server enable`

`undo netconf ssh server enable`

Default

NETCONF over SSH is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This feature allows you to use an SSH client to invoke NETCONF as an SSH subsystem. Then, you can directly use XML messages to perform NETCONF operations without using the **`xml`** command.

Before you execute this command, configure the authentication mode for users as **scheme** on the device. Then, the NETCONF-over-SSH-enabled user terminals can access the device through NETCONF over SSH.

Only capability set **urn:ietf:params:netconf:base:1.0** is available. It is supported by both the device and user terminals.

Examples

Enable NETCONF over SSH.

```
<Sysname> system-view
[Sysname] netconf ssh server enable
```

netconf ssh server port

Use **netconf ssh server port** to specify a port to listen for NETCONF over SSH session requests.

Use **undo netconf ssh server port** to restore the default.

Syntax

netconf ssh server port *port-number*

undo netconf ssh server port

Default

The device uses port 830 to listen for NETCONF over SSH session requests.

Views

System view

Predefined user roles

network-admin

Parameters

*port-numbe*r: Specifies a port by its number in the range of 1 to 65535.

Usage guidelines

Make sure the specified port is not being used by other services.

Examples

Use port 800 to listen for NETCONF over SSH session requests.

```
<Sysname> system-view
[Sysname] netconf ssh server port 800
```

xml

Use **xml** to enter XML view.

Syntax

xml

Views

User view

Predefined user roles

network-admin

network-operator

Usage guidelines

In XML view, use NETCONF messages to configure the device or obtain data from the device. The NETCONF operations you can perform depend on the user roles you have, as shown in Table 2.

Table 2 NETCONF operations available for the predefined user roles

User role	NETCONF operations
network-admin	All NETCONF operations
network-operator	• Get • Get-bulk • Get-bulk-config • Get-config • Get-sessions • Close-session

To ensure the format correctness of NETCONF messages in XML view, do not enter NETCONF messages manually. Copy and paste the messages.

While the device is performing a NETCONF operation, do not perform any other operations, such as pasting a NETCONF message or pressing **Enter**.

For the device to identify NETCONF messages, you must add end mark **]]>]]>** at the end of each NETCONF message.

After you enter XML view, the device automatically advertises its NETCONF capabilities to the client. In response, you must configure the client to notify the device of its supported NETCONF capabilities. After the capability exchange, you can use the client to configure the device.

NETCONF messages must comply with the XML format requirements and semantic and syntactic requirements in the NETCONF XML API reference for the device. As a best practice, use third-party software to generate NETCONF messages to ensure successful configuration.

To quit XML view, use a NETCONF message instead of the **quit** command.

If you have configured a shortcut key (**Ctrl + C**, by default) by using the **escape-key** command in user line/user line class view, the NETCONF message should not contain the shortcut key string. If the NETCONF message contains the shortcut key string, relevant configurations in XML view might be affected. For example, in user line view, you configured "a" as the shortcut key by using the **escape-key a** command. When a NETCONF message includes the character "a," only the contents after the last "a" in the message can be processed.

Examples

Enter XML view.

```
<Sysname> xml
<?xml version="1.0" encoding="UTF-8"?><hello
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"><capabilities><capability>urn:ietf:pa
rams:netconf:base:1.1</capability><capability>urn:ietf:params:netconf:writable-runnin
g</capability><capability>urn:ietf:params:netconf:capability:notification:1.0</capabi
lity><capability>urn:ietf:params:netconf:capability:validate:1.1</capability><capabil
ity>urn:ietf:params:netconf:capability:interleave:1.0</capability><capability>urn:h3c
:params:netconf:capability:h3c-netconf-ext:1.0</capability></capabilities><session-id
>1</session-id></hello>]]>]]>
```

Notify the device of the NETCONF capabilities supported on the client.

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>
```

```
            urn:ietf:params:netconf:base:1.0
    </capability>
  </capabilities>
</hello>]]>]]>
```

Quit XML view.

```
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <close-session/>
</rpc>]]>]]>
<Sysname>
```

Contents

CWMP commands

cwmp

Use **cwmp** to enter CWMP view.

Syntax

cwmp

Views

System view

Predefined user roles

network-admin

Examples

Enter CWMP view.

```
<Sysname> system-view
[Sysname] cwmp
```

Related commands

cwmp enable

cwmp acs default password

Use **cwmp acs default password** to configure a password for authentication to the default ACS URL.

Use **undo cwmp acs default password** to restore the default.

Syntax

cwmp acs default password { **cipher** | **simple** } *string*

undo cwmp acs default password

Default

No password is configured for authentication to the default ACS URL.

Views

CWMP view

Predefined user roles

network-admin

Parameters

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 255 characters. Its encrypted form is a case-sensitive string of 33 to 373 characters.

Usage guidelines

You can configure only one password for authentication to the default ACS URL. If you execute this command multiple times, the most recent configuration takes effect.

For a successful connection, make sure the CPE has the same username and password settings as the ACS.

Examples

Configure the password used for authentication to the default ACS URL.

```
<Sysname> system-view
[Sysname] cwmp
[Sysname-cwmp] cwmp acs default password simple newpsw
```

Related commands

cwmp acs default url

cwmp acs default username

cwmp acs default url

Use **cwmp acs default url** to specify a default ACS URL.

Use **undo cwmp acs default url** to restore the default.

Syntax

cwmp acs default url *url*

undo cwmp acs default url

Default

No default ACS URL is specified.

Views

CWMP view

Predefined user roles

network-admin

Parameters

url: Specifies the default ACS URL, a string of 8 to 255 characters. The URL must use the **http://***host[:port]/path* or **https://***host[:port]/path* format.

Usage guidelines

The CPE attempts to connect to the default ACS URL if no ACS URL has been assigned to it through the **cwmp acs url** command or DHCP.

You can configure only one default ACS URL. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the default ACS URL.

```
<Sysname> system-view
[Sysname] cwmp
[Sysname-cwmp] cwmp acs default url http://www.acs.com:9090
```

Related commands

cwmp acs default password

cwmp acs default username

cwmp acs default username

Use **cwmp acs default username** to configure the username for authentication to the default ACS URL.

Use **undo cwmp acs default username** to restore the default.

Syntax

cwmp acs default username *username*

undo cwmp acs default username

Default

No username is configured for authentication to the default ACS URL.

Views

CWMP view

Predefined user roles

network-admin

Parameters

username: Specifies a username, a case-sensitive string of 1 to 255 characters.

Usage guidelines

You can configure only one username for authentication to the default ACS URL. If you execute this command multiple times, the most recent configuration takes effect.

For a successful connection, make sure the CPE has the same username and password settings as the ACS.

Examples

Configure the username for authentication to the default ACS URL.

```
<Sysname> system-view
[Sysname] cwmp
[Sysname-cwmp] cwmp acs default username newname
```

Related commands

cwmp acs default password

cwmp acs default url

cwmp acs password

Use **cwmp acs password** to configure the password for authentication to the preferred ACS URL.

Use **undo cwmp acs password** to restore the default.

Syntax

cwmp acs password { **cipher** | **simple** } *string*

undo cwmp acs password

Default

No password is configured for authentication to the preferred ACS URL.

Views

CWMP view

Predefined user roles

network-admin

Parameters

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 255 characters. Its encrypted form is a case-sensitive string of 33 to 373 characters.

Usage guidelines

You can configure only one password for authentication to the preferred ACS URL. If you execute this command multiple times, the most recent configuration takes effect.

For a successful connection, make sure the CPE has the same username and password settings as the ACS.

Examples

Configure the password used for authentication to the preferred ACS URL.

```
<Sysname> system-view
[Sysname] cwmp
[Sysname-cwmp] cwmp acs password simple newpsw
```

Related commands

cwmp acs url

cwmp acs username

cwmp acs url

Use **cwmp acs url** to specify a preferred ACS URL.

Use **undo cwmp acs url** to restore the default.

Syntax

cwmp acs url *url*

undo cwmp acs url

Default

No preferred ACS URL is specified.

Views

CWMP view

Predefined user roles

network-admin

Parameters

url: Specifies the preferred ACS URL, a string of 8 to 255 characters. The URL must use the **http://***host[:port]/path* or **https://***host[:port]/path* format.

Usage guidelines

The device supports only one preferred ACS URL. If you execute this command multiple times, the most recent configuration takes effect.

The preferred ACS URL is configurable from the CPE's CLI, the DHCP server, and the ACS. The CLI- and ACS-assigned URLs have higher priority than the DHCP-assigned URL. The CLI- and ACS-assigned URLs overwrite each other.

The CPE uses the default ACS attributes for connection establishment only when it is not assigned a preferred ACS URL from the CLI, ACS, or DHCP server.

Examples

Specify the ACS URL.

```
<Sysname> system-view
[Sysname] cwmp
[Sysname-cwmp] cwmp acs url http://www.acs.com:9090
```

cwmp acs username

Use **cwmp acs username** to configure the username for authentication to the preferred ACS URL.

Use **undo cwmp acs username** to restore the default.

Syntax

cwmp acs username *username*

undo cwmp acs username

Default

No username is configured for authentication to the preferred ACS URL.

Views

CWMP view

Predefined user roles

network-admin

Parameters

username: Specifies a username, a case-sensitive string of 1 to 255 characters.

Usage guidelines

You can configure only one username for authentication to the preferred ACS URL. If you execute this command multiple times, the most recent configuration takes effect.

For a successful connection, make sure the CPE has the same username and password settings as the ACS.

Examples

Configure the username used for authentication to the preferred ACS URL.

```
<Sysname> system-view
[Sysname] cwmp
[Sysname-cwmp] cwmp acs username newname
```

Related commands

cwmp acs password

cwmp cpe connect interface

Use **cwmp cpe connect interface** to specify the CWMP connection interface.

Use **undo cwmp cpe connect interface** to restore the default.

Syntax

cwmp cpe connect interface *interface-type interface-number*

undo cwmp cpe connect interface

Default

No CWMP connection interface is specified.

Views

CWMP view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies the type and number of the CWMP connection interface.

Usage guidelines

A CWMP connection interface is the interface that the CPE uses to communicate with the ACS. To establish a CWMP connection, the CPE sends the IP address of this interface in the Inform message, and the ACS replies to this IP address.

Typically, the CPE selects the CWMP connection interface automatically. If the CWMP connection interface is not the interface that connects the CPE to the ACS, the CPE fails to establish a CWMP connection with the ACS. For example, an incorrect CWMP connection interface selection occurs when the following conditions exist:

- The CPE has multiple Layer 3 interfaces.
- The IP addresses of the CWMP connection interface and the ACS are not in the same subnet.

In this case, you need to use this command to manually specify the CWMP connection interface.

Examples

Specify VLAN-interface 2 as the CWMP connection interface.

```
<Sysname> system-view
[Sysname] cwmp
[Sysname-cwmp] cwmp cpe connect interface vlan-interface 2
```

cwmp cpe connect retry

Use **cwmp cpe connect retry** to set the maximum number of attempts the CPE can make to retry a failed CWMP connection.

Use **undo cwmp cpe connect retry** to restore the default.

Syntax

cwmp cpe connect retry *retries*

undo cwmp cpe connect retry

Default

The CPE retries a failed connection until the connection is established with the ACS.

Views

CWMP view

Predefined user roles

network-admin

Parameters

retries: Specifies the maximum number of CWMP connection retries. The value range is 0 to 100. To disable the CPE to retry a CWMP connection, set this argument to 0.

Usage guidelines

The CPE retries connecting to the ACS when its initial connection attempt fails or the CWMP session is ended before the CPE receives a session closed message from the ACS. The CPE does not stop its connection retry attempts until the connection is established or the number of connection retries reaches the upper limit.

Examples

Set the maximum number of CWMP connection retries to 5.

```
<Sysname> system-view
[Sysname] cwmp
[Sysname-cwmp] cwmp cpe connect retry 5
```

cwmp cpe inform interval

Use **cwmp cpe inform interval** to set the periodic Inform interval.

Use **undo cwmp cpe inform interval** to restore the default.

Syntax

cwmp cpe inform interval *interval*

undo cwmp cpe inform interval

Default

The periodic Inform interval is 600 seconds.

Views

CWMP view

Predefined user roles

network-admin

Parameters

interval: Sets the periodic Inform interval in the range of 10 to 86400 seconds.

Usage guidelines

This command sets the interval for the CPE to send Inform messages automatically to the ACS. For the command to take effect, you must configure the **cwmp cpe inform interval enable** command.

Examples

Set the periodic Inform interval to 3600 seconds.

```
<Sysname> system-view
```

```
[Sysname] cwmp
[Sysname-cwmp] cwmp cpe inform interval enable
[Sysname-cwmp] cwmp cpe inform interval 3600
```

Related commands

cwmp cpe inform interval enable

cwmp cpe inform interval enable

Use **cwmp cpe inform interval enable** to enable the periodic Inform feature.

Use **undo cwmp cpe inform interval enable** to disable the periodic Inform feature.

Syntax

cwmp cpe inform interval enable

undo cwmp cpe inform interval enable

Default

The CPE does not send Inform messages periodically.

Views

CWMP view

Predefined user roles

network-admin

Usage guidelines

If this command is configured, the CPE sends Inform messages regularly to establish a CWMP session with the ACS. To set the periodic Inform interval, use the **cwmp cpe inform interval** command.

Examples

Enable the periodic Inform feature.

```
<Sysname> system-view
[Sysname] cwmp
[Sysname-cwmp] cwmp cpe inform interval enable
```

Related commands

cwmp cpe inform interval

cwmp cpe inform time

Use **cwmp cpe inform time** to schedule a connection initiation for the CPE to connect to the ACS.

Use **undo cwmp cpe inform time** to restore the default.

Syntax

cwmp cpe inform time *time*

undo cwmp cpe inform time

Default

No connection initiation has been scheduled.

Views

CWMP view

Predefined user roles

network-admin

Parameters

time: Specifies the time at which the CPE sends an Inform message. The time format is *yyyy-mm-dd*T*hh:mm:ss*, and the value range is 1970-01-01T00:00:00 to 2035-12-31T23:59:59. The specified time must be greater than the current system time.

Examples

Configure the CPE to send an Inform message at 2007-12-01T20:00:00.

```
<Sysname> system-view
[Sysname] cwmp
[Sysname-cwmp] cwmp cpe inform time 2012-12-01T20:00:00
```

cwmp cpe password

Use **cwmp cpe password** to configure the password for the CPE to authenticate the ACS.

Use **undo cwmp cpe password** to restore the default.

Syntax

cwmp cpe password { **cipher** | **simple** } *string*

undo cwmp cpe password

Default

No password is configured for authenticating the ACS.

Views

CWMP view

Predefined user roles

network-admin

Parameters

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 255 characters. Its encrypted form is a case-sensitive string of 33 to 373 characters.

Usage guidelines

You can configure only one password for the ACS to authenticate to the CPE when it initiates a connection. If you execute this command multiple times, the most recent configuration takes effect.

For a successful connection, make sure the ACS has the same username and password settings as the CPE.

If a password is configured, the ACS must provide the correct password when it initiates a connection to the CPE. If the password is incorrect, the CPE denies the connection request from the ACS.

You do not need to configure this command if you want to authenticate the ACS only based on its username.

Examples

Configure the password used for authenticating the ACS.

```
<Sysname> system-view
[Sysname] cwmp
[Sysname-cwmp] cwmp cpe password simple newpsw
```

Related commands

cwmp cpe username

cwmp cpe provision-code

Use **cwmp cpe provision-code** to configure the provision code of the CPE.

Use **undo cwmp cpe provision-code** to restore the default.

Syntax

cwmp cpe provision-code *provision-code*

undo cwmp cpe provision-code

Default

The provision code is **PROVISIONINGCODE**.

Views

CWMP view

Predefined user roles

network-admin

Parameters

provision-code: Specifies a provision code, a string of 1 to 64 characters. The string can contain uppercase letters, digits, and the full stop (.).

Usage guidelines

The ACS can use the provision code to identify services assigned to each CPE. For correct configuration deployment, make sure the same provision code is configured on the CPE and the ACS. For information about the support of your ACS for provision codes, see the ACS documentation.

The CPE can have only one provision code. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the provision code to **ABC20150714**.

```
<Sysname> system
[Sysname] cwmp
[Sysname-cwmp] cwmp cpe provision-code ABC20150714
```

cwmp cpe stun enable

Use **cwmp cpe stun enable** to enable NAT traversal for the connection requests from the ACS to reach the CPE through a NAT gateway.

Use **undo cwmp cpe stun enable** to disable NAT traversal for the connection requests from the ACS to reach the CPE through a NAT gateway.

Syntax

cwmp cpe stun enable

undo cwmp cpe stun enable

Default

NAT traversal is disabled for CWMP.

Views

CWMP view

Predefined user roles

network-admin

Usage guidelines

Connection requests initiated from the CPE can reach the ACS through a NAT gateway without NAT traversal. However, for the connection request initiated from the ACS to reach the CPE, you must enable NAT traversal on the CPE when a NAT gateway resides between the CPE and the ACS.

The NAT traversal feature complies with *Simple Traversal of UDP Through NATs (STUN)*, RFC 3489. The feature enables the CPE to do the following:

- Discovers the NAT gateway.
- Obtains an open NAT binding (a public IP address and port binding) through which the ACS can send unsolicited packets.

The CPE sends the binding to the ACS when it initiates a connection to the ACS. For the connection requests sent by the ACS at any time to reach the CPE, the CPE maintains the open NAT binding.

Examples

Enable NAT traversal for the CPE.

```
<Sysname> system-view
[Sysname] cwmp
[Sysname-cwmp] cwmp cpe stun enable
```

cwmp cpe username

Use **cwmp cpe username** to configure the username for the CPE to authenticate the ACS.

Use **undo cwmp cpe username** to restore the default.

Syntax

cwmp cpe username *username*

undo cwmp cpe username

Default

No username is configured for authenticating the ACS.

Views

CWMP view

Predefined user roles

network-admin

Parameters

username: Specifies a username, a case-sensitive string of 1 to 255 characters.

Usage guidelines

You can configure only one username for the ACS to authenticate to the CPE when it initiates a connection. If you execute this command multiple times, the most recent configuration takes effect.

For a successful connection, make sure the ACS has the same username setting as the CPE. If a password is required, you must also make sure the ACS has the same password setting as the CPE.

The ACS must provide the correct username when it initiates a connection to the CPE. If the username is incorrect, the CPE denies the connection request from the ACS.

Examples

Configure the username used for authenticating the ACS.

```
<Sysname> system-view
[Sysname] cwmp
[Sysname-cwmp] cwmp cpe username newname
```

Related commands

cwmp cpe password

cwmp cpe wait timeout

Use **cwmp cpe wait timeout** to set the close-wait timer for the CPE to close an idle connection.

Use **undo cwmp cpe wait timeout** to restore the default.

Syntax

cwmp cpe wait timeout *seconds*

undo cwmp cpe wait timeout

Default

The close-wait timer is 30 seconds.

Views

CWMP view

Predefined user roles

network-admin

Parameters

seconds: Sets the close-wait timer, in the range of 30 to 1800 seconds.

Usage guidelines

The close-wait timer has the following functions:

- It specifies the amount of time the connection to the ACS can be idle before it is terminated. The CPE terminates the connection to the ACS if no traffic is transmitted before the timer expires.
- It also specifies the amount of time the CPE waits for the response to a session request. The CPE determines that its session attempt has failed when the timer expires. By default, the CPE retries a failed session until the session is established with the ACS. To limit the number of retries, use the **cwmp cpe connect retry** command.

Examples

Set the close-wait time to 60 seconds.

```
<Sysname> system-view
```

```
[Sysname] cwmp
[Sysname-cwmp] cwmp cpe wait timeout 60
```

Related commands

cwmp cpe connect retry

cwmp enable

Use **cwmp enable** to enable CWMP.

Use **undo cwmp enable** to disable CWMP.

Syntax

cwmp enable

undo cwmp enable

Default

CWMP is disabled.

Views

CWMP view

Predefined user roles

network-admin

Usage guidelines

CWMP configuration takes effect only after CWMP is enabled.

Examples

Enable CWMP.

```
<Sysname> system-view
[Sysname] cwmp
[Sysname-cwmp] cwmp enable
```

Related commands

cwmp

display cwmp configuration

Use **display cwmp configuration** to display the CWMP configuration.

Syntax

display cwmp configuration

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the CWMP configuration after CWMP is enabled.

```
<Sysname> display cwmp configuration
```

```
CWMP state                    : Enabled
ACS URL                       : http://www.acs.com:9090
ACS username                  : newname
ACS default URL               : Null
ACS default username          : defname
Periodic inform               : Disabled
Inform interval               : 600s
Inform time                   : None
Wait timeout                  : 30s
Connection retries            : Unlimited
Source IP interface           : None
STUN state                    : Disabled
SSL policy name               : Null
```

Table 1 Command output

Field	Description
CWMP state	Status of CWMP: **Enabled** or **Disabled**.
ACS URL	Preferred ACS URL. This field displays **Null** if no preferred ACS URL has been specified.
ACS username	Username for the CPE to authenticate to the ACS. This field displays **Null** if no username has been configured for authentication to the preferred ACS URL.
ACS default URL	Default ACS URL. This field displays **Null** if no default ACS URL has been configured.
ACS default username	Username for the CPE to authenticate to the default ACS URL. This field displays **Null** if no username has been configured for authentication to the default ACS URL.
Periodic inform	Status of the periodic Inform feature: **Enabled** or **Disabled**.
Inform interval	Periodic Inform interval. The default interval is 600 seconds.
Inform time	Date and time at which an Inform message is scheduled to be sent. If you do not schedule an Inform sending, this field displays **None**.
Wait timeout	Close-wait timer. This timer is configurable with the **cwmp cpe wait timeout** command.
Connection retries	Number of attempts the CPE can make to retry a failed CWMP connection. This field displays **Unlimited** if the default setting is used. The CPE retries a failed session until the session is established with the ACS.
Source IP interface	IP address of the specified CWMP connection interface. This field displays **None** if you have not specified a CWMP connection interface.
STUN state	Status of NAT traversal for CWMP: **Enabled** or **Disabled**.
SSL policy name	SSL client policy specified for the CPE to authenticate the ACS for establishing an HTTPS connection. You must specify an SSL client policy when HTTPS is used. This field displays **Null** if you have not specified an SSL client policy.

Related commands

display cwmp status

display cwmp status

Use **display cwmp status** to display CWMP state information.

Syntax

display cwmp status

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display CWMP state information.

```
<Sysname> display cwmp status
CWMP state                                  : Enabled
ACS URL of most recent connection           : http://www.acs.com:9090
ACS information source                      : User
ACS username of most recent connection      : newname
Connection status                           : Disconnected
Data transfer status                        : None
Most recent successful connection attempt   : None
Length of time before next connection attempt : 1096832s
```

Table 2 Command output

Field	Description
CWMP state	Status of CWMP: **Enabled** or **Disabled**.
ACS URL of most recent connection	ACS URL used for the most recent connection attempt. This field displays **Null** if no ACS URL was available.
ACS information source	Source from which the CPE obtained the ACS URL: • **User**—ACS URL assigned by using the **cwmp acs url** command or by ACS. • **DHCP**—ACS URL assigned by the DHCP server. • **Default**—ACS URL assigned by using the **cwmp acs default url** command. This field displays **None** if no ACS URL was available.
ACS username of most recent connection	Username used for the most recent connection to the ACS. This field displays **Null** if no ACS username was available.
Connection status	Current CWMP session status: • **Connected**—A CWMP session has been established to the ACS. • **Disconnected**—No CWMP session has been established to the ACS. • **Waiting response**—The CPE is waiting for the connection response from the ACS.
Data transfer status	Data transfer status of the CPE: • **Uploading**—The CPE is uploading data. • **Downloading**—The CPE is downloading data. • **None**—No data is transferred.

Field	Description
Most recent successful connection attempt	Time of the most recent successful CWMP connection. This field displays **None** if no CWMP session was established.
Length of time before next connection attempt	Amount of time (in seconds) that the CPE must wait before it initiates the next connection. This field displays **None** if the CPE does not detect an event that will trigger a connection attempt.

Related commands

display cwmp configuration

ssl client-policy

Use **ssl client-policy** to specify an SSL client policy for CWMP.

Use **undo ssl client-policy** to restore the default.

Syntax

ssl client-policy *policy-name*

undo ssl client-policy

Default

No SSL client policy is specified for CWMP.

Views

CWMP view

Predefined user roles

network-admin

Parameters

policy-name: Specifies the name of an SSL client policy, a string of 1 to 31 characters.

Usage guidelines

CWMP uses HTTP or HTTPS for data transmission. If the ACS uses HTTPS for secure access, its URL begins with **https://**. You must configure an SSL client policy for the CPE to authenticate the ACS for establishing an HTTPS connection. For more information about configuring SSL client policies, see *Security Configuration Guide*.

Examples

Specify the SSL client policy **test** for CWMP.

```
<Sysname> system
[Sysname] cwmp
[Sysname-cwmp] ssl client-policy test
```

Contents

EAA commands

action cli

Use **action cli** to add a CLI action to a monitor policy.

Use **undo action** to remove an action.

Syntax

action *number* **cli** *command-line*

undo action *number*

Default

A monitor policy does not contain any actions.

Views

CLI-defined policy view

Predefined user roles

network-admin

Parameters

number: Specifies an action ID in the range of 0 to 231.

cli *command-line*: Specifies the command line to be executed when the event occurs. You can enter abbreviated forms of command keywords, but you must make sure the forms can uniquely identify the command keywords. For example, you can enter **int loop 1** for the **interface loopback 1** command.

Usage guidelines

You can configure a series of actions to be executed in response to the event specified in a monitor policy. EAA executes the actions in ascending order of action IDs. When you add actions to a policy, you must make sure the execution order is correct. If two actions have the same ID, the most recent one takes effect.

To execute a command in a view other than user view, you must define actions required for accessing the target view before defining the command execution action. In addition, you must number the actions in the order they should be executed, starting with entering system view.

For example, to shut down an interface, you must create the following actions in order:

1. Action to enter system view.
2. Action to enter interface view.
3. Action to shut down the interface.

When you define an action, you can specify a value or specify a variable name for an argument. For more information about using EAA environment variables, see "rtm environment."

Examples

Configure a CLI action for the CLI-defined policy **test** to shut down GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] action 1 cli system-view
[Sysname-rtm-test] action 2 cli interface gigabitethernet 1/0/1
[Sysname-rtm-test] action 3 cli shutdown
```

action reboot

Use **action reboot** to add a reboot action to a monitor policy.

Use **undo action** to remove an action.

Syntax

action *number* **reboot** [**slot** *slot-number*]

undo action *number*

Default

A monitor policy does not contain any actions.

Views

CLI-defined policy view

Predefined user roles

network-admin

Parameters

number: Specifies an action ID in the range of 0 to 231.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, the command reboots the IRF fabric.

Usage guidelines

The reboot action configured with this command reboots devices without saving the running configuration. If you want to save the running configuration, use the **action cli** command to configure reboot actions.

You can configure a series of actions to be executed in response to the event specified in a monitor policy. EAA executes the actions in ascending order of action IDs. When you add actions to a policy, you must make sure the execution order is correct. If two actions have the same ID, the most recent one takes effect.

When you define an action, you can specify a value or specify a variable name for an argument. For more information about using EAA environment variables, see "rtm environment."

Examples

Configure an action for the CLI-defined policy **test** to reboot the specified slot.

<Sysname> system-view

```
[Sysname] rtm cli-policy test
[Sysname-rtm-test] action 3 reboot slot 1
```

action switchover

Use **action switchover** to add an active/standby switchover action to a monitor policy.

Use **undo action** to remove an action.

Syntax

action *number* **switchover**

undo action *number*

Default

A monitor policy does not contain any actions.

Views

CLI-defined policy view

Predefined user roles

network-admin

Parameters

number: Specifies an action ID in the range of 0 to 231.

Usage guidelines

You can configure a series of actions to be executed in response to the event specified in a monitor policy. EAA executes the actions in ascending order of action IDs. When you add actions to a policy, you must make sure the execution order is correct. If two actions have the same ID, the most recent one takes effect.

This command does not trigger a master/subordinate switchover in either of the following situations:

- No subordinate device is configured.
- The subordinate device is not in up state.

Examples

Configure an action for the CLI-defined policy **test** to perform an active/standby switchover.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] action 3 switchover
```

action syslog

Use **action syslog** to add a Syslog action to a monitor policy.

Use **undo action** to remove an action.

Syntax

action *number* **syslog priority** *priority* **facility** *local-number* **msg** *msg-body*

undo action *number*

Default

A monitor policy does not contain any actions.

Views

CLI-defined policy view

Predefined user roles

network-admin

Parameters

number: Specifies an action ID in the range of 0 to 231.

priority *priority*: Specifies the log severity level in the range of 0 to 7. A lower value represents a higher severity level.

facility *local-number*: Specifies a logging facility by its facility number in the range of local0 to local7. Facility numbers are used by a log host to identify log creation facilities for filtering log messages.

msg *msg-body*: Configures the log message body.

Usage guidelines

EAA sends log messages to the information center. You can configure the information center to output these messages to certain destinations. For more information about the information center, see "Configuring the information center."

You can configure a series of actions to be executed in response to the event specified in a monitor policy. EAA executes the actions in ascending order of action IDs. When you add actions to a policy, you must make sure the execution order is correct. If two actions have the same ID, the most recent one takes effect.

When you define an action, you can specify a value or specify a variable name for an argument. For more information about using EAA environment variables, see "rtm environment."

Examples

Configure an action for the CLI-defined policy **test** to send a log message "hello" with a severity of 7 from the facility device **local3**.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] action 3 syslog priority 7 facility local3 msg hello
```

commit

Use **commit** to enable a CLI-defined monitor policy.

Syntax

commit

Default

No CLI-defined monitor policies are enabled.

Views

CLI-defined policy view

Predefined user roles

network-admin

Usage guidelines

You must execute this command for a CLI-defined monitor policy to take effect.

After changing the settings in a policy that has been enabled, you must re-execute this command for the changes to take effect.

Examples

Enable CLI-defined monitor policy **test**.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] commit
```

display rtm environment

Use **display rtm environment** to display user-defined EAA environment variables and their values.

Syntax

display rtm environment [*var-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

var-name: Specifies a user-defined EAA environment variable by its name, a case-sensitive string of 1 to 63 characters. The name can contain digits, letters, and the underscore sign (_), but its leading character cannot be the underscore sign. If you do not specify a variable, this command displays all user-defined EAA environment variables.

Examples

Display all user-defined EAA environment variables.

```
<Sysname> display rtm environment
Name             Value
save_cmd         save main force
show_run_cmd     display current-configuration
```

Table 1 Command output

Field	Description
Name	Name of a user-defined EAA environment variable. This field displays a maximum of 30 characters. To display a user-defined EAA environment variable name of more than 30 characters, use the **display current-configuration** command.
Value	Value of the user-defined EAA environment variable. This field displays a maximum of 30 characters. To display a user-defined EAA environment variable value of more than 30 characters, use the **display current-configuration** command.

display rtm policy

Use **display rtm policy** to display information about EAA monitor policies.

Syntax

display rtm policy { **active** | **registered** [**verbose**] } [*policy-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

active: Specifies policies that are executing the actions.

registered: Specifies policies that have been created.

verbose: Displays detailed information about monitor policies.

policy-name: Specifies a policy by its name, a case-sensitive string of 1 to 63 characters. If you do not specify a policy, the command displays information about all monitor policies.

Usage guidelines

To display the running configuration of CLI-defined monitor policies, execute the **display current-configuration** command in any view or execute the **display this** command in CLI-defined monitor policy view.

Examples

Display monitor policies that are executing the actions.

```
<Sysname> display rtm policy active
JID   Type  Event      TimeActive           PolicyName
507   CLI   INTERFACE  Aug 29 14:55:55 2013 test
```

Table 2 Command output

Field	Description
JID	Job ID, displayed only when you specify the **active** keyword.
Type	Policy creation method: • **TCL**—The policy was configured by using Tcl. • **CLI**—The policy was configured from the CLI.
Event	Event type, including CLI, hotplug, interface, process, SNMP, SNMP-Notification, Syslog, and track.
TimeActive	Time when the monitor policy was triggered.
PolicyName	Name of the monitor policy.

Display brief information about all created monitor policies.

```
<Sysname> display rtm policy registered
Total number: 1
Type  Event      TimeRegistered       PolicyName
CLI              Aug 29 14:54:50 2013 test
```

Table 3 Command output

Field	Description
Total number	Total number of the monitor policies.
Type	Policy creation method: • **TCL**—The policy was configured by using Tcl. • **CLI**—The policy was configured from the CLI.
Event	Event type, including CLI, hotplug, interface, process, SNMP, SNMP-Notification, Syslog, and track.
TimeRegistered	Time when the monitor policy was created.
PolicyName	Name of the monitor policy.

Display detailed information about all monitor policies.

```
<Sysname> display rtm policy registered verbose
  Total number: 1

   Policy Name: test
   Policy Type: CLI
    Event Type:
TimeRegistered: Aug 29 14:54:50 2013
```

```
User-role: network-operator
           network-admin
```

Table 4 Command output

Field	Description
Total number	Total number of the monitor polices.
PolicyName	Name of the monitor policy.
Policy Type	Policy creation method: • **TCL**—The policy was configured by using Tcl. • **CLI**—The policy was configured from the CLI.
Event Type	Event type, including CLI, hotplug, interface, process, SNMP, SNMP-Notification, Syslog, and track.
TimeRegistered	Time when the policy was created.
User-role	User roles for executing the monitor policy. To execute the monitor policy, an administrator must have a minimum of one of the displayed user roles.

event cli

Use **event cli** to configure a CLI event for a CLI-defined monitor policy.

Use **undo event** to delete the event in a CLI-defined monitor policy.

Syntax

event cli { **async** [**skip**] | **sync** } **mode** { **execute** | **help** | **tab** } **pattern** *regular-exp*

undo event

Default

No CLI event is configured.

Views

CLI-defined policy view

Predefined user roles

network-admin

Parameters

async [**skip**]: Enables or disables the system to execute the command that triggers the policy. If you specify the **skip** keyword, the system executes the actions in the policy without executing the command that triggers the policy. If you do not specify the **skip** keyword, the system executes both the actions in the policy and the command entered at the CLI.

sync: Enables the system to execute the command that triggers the event only if the policy has been executed successfully.

mode { **execute** | **help** | **tab** }: Specifies the CLI operation to monitor:

- **execute**: Triggers the policy when a matching command is entered.
- **help**: Triggers the policy when a question mark (?) is entered at a matching command line.
- **tab**: Triggers the policy when the **Tab** key is pressed to complete a parameter in a matching command line.

pattern *regular-exp*: Specifies a regular expression for matching commands that trigger the policy. For more information about using regular expressions, see CLI in *Fundamentals Configuration Guide*.

Usage guidelines

Use CLI event monitor policies to monitor operations performed at the CLI.

You can configure only one event for a monitor policy. If the monitor policy already contains an event, the new event replaces the old event.

Examples

Configure a CLI-defined policy to monitor execution of commands that contain the **display interface brief** string. Enable the system to execute the actions in the policy without executing the command that triggers the policy.

```
<Sysname>system-view
[Sysname] rtm cli-policy test
[Sysname-rmt-test] event cli async skip mode execute pattern display interface brief
```

Configure a CLI-defined policy to monitor the use of the **Tab** key at command lines that contain the **display interface brief** string. Enable the system to execute the actions in the policy and display the complete parameter when **Tab** is pressed at a policy-matching command line.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rmt-test] event cli async mode tab pattern display interface brief
```

Configure a CLI-defined policy to monitor the use of the question mark (?) at command lines that contain the **display interface brief** string. Enable the system to execute a policy-matching command line only if the actions in the policy are executed successfully when a question mark is entered at the command line.

```
<Sysname>system-view
[Sysname] rtm cli-policy test
[Sysname-rmt-test] event cli sync mode help pattern display interface brief
```

event hotplug

Use **event hotplug** to configure a hot-swapping event.

Use **undo event** to delete the event in a CLI-defined monitor policy.

Syntax

event hotplug [**insert** | **remove**] **slot** *slot-number*

undo event

Default

No hotplug event is configured.

Views

CLI-defined policy view

Predefined user roles

network-admin

Parameters

insert: Specifies the IRF member device join event.

remove: Specifies the IRF member device leave event.

slot *slot-number*: Specifies an IRF member device by its member ID.

Usage guidelines

After you configure the event, the monitor policy is triggered when the member device joins or leaves the IRF fabric. If you do not specify the **insert** or **remove** keyword, EAA monitors the member device for joining or leaving the IRF fabric.

You can configure only one event entry for a monitor policy. If the monitor policy already contains an event entry, the new event entry replaces the old event entry.

Examples

Configure a CLI-defined policy to monitor the member device for joining or leaving the IRF fabric.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] event hotplug slot 1
```

event interface

Use **event interface** to configure an interface event for a CLI-defined monitor policy.

Use **undo event** to delete the event in a CLI-defined monitor policy.

Syntax

event interface *interface-list* **monitor-obj** *monitor-obj* **start-op** *start-op* **start-val** *start-val* **restart-op** *restart-op* **restart-val** *restart-val* [**interval** *interval*]

undo event

Default

No interface event is configured.

Views

CLI-defined policy view

Predefined user roles

network-admin

Parameters

interface-list: Specifies a space-separated list of up to eight interface items. An item specifies an interface or specifies a range of interfaces in the form of *interface-type interface-number* **to** *interface-type interface-number*. The interfaces in an interface range must be same type. The start interface number must be smaller than the end interface number.

monitor-obj *monitor-obj*: Specifies the traffic statistic to be monitored on the interface. For keywords available for the *monitor-obj* argument, see Table 5.

start-op *start-op*: Specifies the operator for comparing the monitored traffic statistic with the start threshold. The start threshold is crossed if the comparison result meets the condition. For keywords available for the *start-op* argument, see Table 6.

start-val *start-val*: Specifies the start threshold to be compared with the monitored traffic statistic. The value range is 0 to 4294967295.

restart-op *restart-op*: Specifies the operator for comparing the monitored traffic statistic with the restart threshold. The restart threshold is crossed if the comparison result meets the condition. For keywords available for the *restart-op* argument, see Table 6.

restart-val *restart-val*: Specifies the restart threshold to be compared with the monitored traffic statistic. The value range is 0 to 4294967295.

interval *interval*: Specifies the interval to sample the monitored traffic statistic for a comparison. The value range is 1 to 4294967295, in seconds. The default value is 300.

Table 5 Monitored objects

Monitored traffic statistic	Description
input-drops	Number of discarded incoming packets during the sampling interval
input-errors	Number of incoming error packets during the sampling interval
output-drops	Number of discarded outgoing packets during the sampling interval
output-errors	Number of outgoing error packets during the sampling interval
rcv-bps	Receive rate, in bps during the sampling interval
rcv-broadcasts	Number of incoming broadcasts during the sampling interval
rcv-kbps	Receive rate, in kilobytes per second
rcv-kpps	Receive rate, in kilopackets per second
rcv-pps	Receive rate, in packets per second
tx-bps	Transmit rate, in bps
tx-kbps	Transmit rate, in kilobytes per second
tx-kpps	Transmit rate, in kilopackets per second
tx-pps	Transmit rate, in packets per second

Table 6 Comparison operators

Comparison operator	Description
eq	Equal to
ge	Greater than or equal to
gt	Greater than
le	Less than or equal to
lt	Less than
ne	Not equal to

Usage guidelines

Use interface event monitor policies to monitor traffic statistics on an interface.

You can configure only one event for a monitor policy. If the monitor policy already contains an event, the new event replaces the old event.

EAA executes an interface event policy when the monitored interface traffic statistic crosses the start threshold in the following situations:

- The statistic crosses the start threshold for the first time.
- The statistic crosses the start threshold each time after it crosses the restart threshold.

The following is the interface event monitor process of EAA:

1. Compares the traffic statistic sample with the start threshold at sampling intervals until the start threshold is crossed.

2. Executes the policy.
3. Compares the traffic statistic sample with the restart threshold at sampling intervals until the restart threshold is crossed.
4. Compares the traffic statistic sample with the start threshold at sampling intervals until the start threshold is crossed.
5. Executes the policy again.

This process cycles for the monitor policy to be executed and re-executed.

Examples

Configure a CLI-defined policy to monitor the incoming error packet statistic on GigabitEthernet 1/0/1 every 60 seconds. Set the start threshold to 1000 and the restart threshold to 50. Enable EAA to execute the policy when the statistic exceeds 1000 for the first time. Enable EAA to re-execute the policy if the statistic exceeds 1000 each time after the statistic has dropped below 50.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] event interface gigabitethernet 1/0/1 monitor-obj input-errors
start-op gt start-val 1000 restart-op lt restart-val 50 interval 60
```

event process

Use **event process** to configure a process event for a CLI-defined monitor policy.

Use **undo event** to delete the event in a CLI-defined monitor policy.

Syntax

event process { **exception** | **restart** | **shutdown** | **start** } [**name** *process-name* [**instance** *instance-id*]] [**slot** *slot-number*]

undo event

Default

No process event is configured.

Views

CLI-defined policy view

Predefined user roles

network-admin

Parameters

exception: Monitors the specified process for exceptional events. EAA executes the policy when an exception occurs to the monitored process.

restart: Monitors the specified process for restart events. EAA executes the policy when the monitored process restarts.

shutdown: Monitors the specified process for shutdown events. EAA executes the policy when the monitored process is shut down.

start: Monitors the specified process for start events. EAA executes the policy when the monitored process starts.

name *process-name*: Specifies a user-mode process by its name. The process can be one that is running or not running. If you do not specify a name, this command monitors all use-mode processes.

instance *instance-id*: Specifies a process instance ID in the range of 0 to 4294967295. The instance ID can be one that has not been created yet. If you do not specify an instance, EAA monitors all instances of the process.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command applies to the IRF fabric.

Usage guidelines

Use process event monitor policies to monitor process state changes. These changes can result from manual operations or automatic system operations.

You can configure only one event for a monitor policy. If the monitor policy already contains an event, the new event replaces the old event.

Examples

Configure a CLI-defined policy to monitor all instances of the process **snmpd** for restart events.

```
<Sysname>system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] event process restart name snmpd
```

event snmp oid

Use **event snmp oid** to configure an SNMP event for a CLI-defined monitor policy.

Use **undo event** to delete the event in a CLI-defined monitor policy.

Syntax

event snmp oid *oid* **monitor-obj** { **get** | **next** } **start-op** *start-op* **start-val** *start-val* **restart-op** *restart-op* **restart-val** *restart-val* [**interval** *interval*]

undo event

Default

No SNMP event is configured.

Views

CLI-defined policy view

Predefined user roles

network-admin

Parameters

oid *oid*: Specifies the OID of the monitored MIB variable, a string of 1 to 256 characters.

monitor-obj { **get** | **next** }: Specifies the SNMP operation used for sampling variable values. The **get** keyword represents the SNMP get operation, and the **next** keyword represents the SNMP getNext operation.

start-op *start-op*: Specifies the operator for comparing the sampled value with the start threshold. The start threshold is crossed if the comparison result meets the condition. For keywords available for the *start-op* argument, see Table 6.

start-val *start-val*: Specifies the start threshold to be compared with the sampled value. The *start-val* argument can be any data type supported by SNMP, including numerals and character strings. The value range for the *start-val* argument is a string of 1 to 512 characters. If the threshold value contains spaces, you must enclose the value in quotation marks (" ").

restart-op *op*: Specifies the operator for comparing the sampled value with the restart threshold. The restart threshold is crossed if the comparison result meets the condition. For keywords available for the *start-op* argument, see Table 6.

restart-op *restart-val*: Specifies the restart threshold to be compared with the sampled value. The *restart-val* argument can be any data type supported by SNMP, including numerals and character strings. The value range for the *restart-val* argument is a string of 1 to 512 characters. If the threshold value contains spaces, you must enclose the value in quotation marks (" ").

interval *interval*: Specifies the sampling interval in the range of 1 to 4294967295, in seconds. The default value is 300.

Usage guidelines

Use SNMP event monitor policy to monitor value changes of MIB variables.

You can configure only one event for a monitor policy. If the monitor policy already contains an event, the new event replaces the old event.

EAA executes an SNMP event policy when the monitored MIB variable's value crosses the start threshold in the following situations:

- The monitored variable's value crosses the start threshold for the first time.
- The monitored variable's value crosses the start threshold each time after it crosses the restart threshold.

The following is the SNMP event monitor process of EAA:

1. Compares the variable sample with the start threshold at sampling intervals until the start threshold is crossed.
2. Executes the policy.
3. Compares the variable sample with the restart threshold at sampling intervals until the restart threshold is crossed.
4. Compares the variable sample with the start threshold at sampling intervals until the start threshold is crossed.
5. Executes the policy again.

This process cycles for the monitor policy to be executed and re-executed.

For the command to take effect, enable SNMP before you execute this command.

Examples

Configure a CLI-defined policy to get the value of the MIB variable **1.3.6.4.9.9.42.1.2.1.6.4** every five seconds. Set the start threshold to 1 and the restart threshold to 2. Enable EAA to execute the policy when the value changes to 1 for the first time. Enable EAA to re-execute the policy if the value changes to 1 each time after the value has changed to 2.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] event snmp oid 1.3.6.4.9.9.42.1.2.1.6.4 monitor-obj get start-op eq
start-val 1 restart-op eq restart-val 2 interval 5
```

event snmp-notification

Use **event snmp-notification** to configure an SNMP-Notification event for a CLI-defined policy.

Use **undo event** to remove the event in a CLI-defined policy.

Syntax

event snmp-notification oid *oid* **oid-val** *oid-val* **op** *op* [**drop**]

undo event

Default

No SNMP-Notification event is configured.

Views

CLI-defined policy view

Predefined user roles

network-admin

Parameters

oid *oid*: Specifies the OID of the monitored MIB variable, a string of 1 to 256 characters.

oid-val *oid-val*: Specifies the threshold to be compared with the sampled value. The *oid-val* argument can be any data type supported by SNMP, including numerals and character strings. The value range for the *oid-val* argument is a string of 1 to 512 characters. If the threshold value contains spaces, you must enclose the value in quotation marks (" ").

op *op*: Specifies the operator for comparing the sampled value with the threshold. The policy is executed if the comparison result meets the condition. For keywords available for the *start-op* argument, see Table 6.

drop: Drops the notification if the comparison result meets the condition. If you do not specify this keyword, the system sends the notification.

Usage guidelines

Use SNMP-Notification event monitor policies to monitor variables in SNMP notifications.

EAA executes an SNMP-Notification event monitor policy when the value of the monitored variable in an SNMP notification meets the specified condition.

You can configure only one event for a monitor policy. If the monitor policy already contains an event, the new event replaces the old event.

For the command to take effect, enable SNMP before you execute this command.

Examples

Configure a CLI-defined policy to monitor SNMP notifications that contain the use name variable **1.3.6.1.4.1.25506.2.2.1.1.2.1.0**. Enable the system to execute the policy and drop the SNMP notification if the use name variable value is **admin**.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] event snmp-notification oid 1.3.6.1.4.1.25506.2.2.1.1.2.1.0 oid-val
admin op eq drop
```

event syslog

Use **event syslog** to configure a Syslog event for a CLI-defined monitor policy.

Use **undo event** to delete the event in a CLI-defined monitor policy.

Syntax

event syslog priority { *priority* | **all** } **msg** *msg* **occurs** *times* **period** *period*

undo event

Default

No Syslog event is configured.

Views

CLI-defined policy view

Predefined user roles

network-admin

Parameters

priority { *priority* | **all** }: Specifies the severity level for matching log messages.

- *priority*: Specifies the lowest severity level for matching log messages. It is an integer in the range of 0 to 7. A lower number represents higher severity level. For example, specify a severity level of 3 to match log messages from level 3 to level 0.
- **all:** Represents any severity level from 0 to 7.

msg msg: Specifies a regular expression to match the logs. The *msg* argument represents a regular expression, a string of 1 to 255 characters.

occurs *times* **period** *period*: Executes the policy if the number of log matches over an interval exceeds the limit. The *times* argument specifies the maximum number of log matches in the range of 1 to 32. The *period* argument specifies an interval in the range of 1 to 4294967295 seconds.

Usage guidelines

Use Syslog event monitor policies to monitor log messages.

EAA executes a Syslog event monitor policy when the number of matching logs over an interval reaches the limit.

NOTE:

EAA does not count log messages generated by the RTM module when it counts log matches.

You can configure only one event for a monitor policy. If the monitor policy already contains an event, the new event replaces the old event.

A regular expression can contain the special characters described in Table 7.

Table 7 Special characters supported in a regular expression

Characters	Meaning	Examples
^	Matches the beginning of a line.	"^u" matches all lines beginning with "u". A line beginning with "Au" is not matched.
$	Matches the end of a line.	"u$" matches all lines ending with "u". A line ending with "uA" is not matched.
. (period)	Matches any single character.	".s" matches "as" and "bs".
*	Matches the preceding character or string zero, one, or multiple times.	"zo*" matches "z" and "zoo", and "(zo)*" matches "zo" and "zozo".
+	Matches the preceding character or string one or multiple times.	"zo+" matches "zo" and "zoo", but not "z".
|	Matches the preceding or succeeding string.	"def|int" matches a line containing "def" or "int".
( )	Matches the string in the parentheses, usually used together with the plus sign (+) or asterisk sign (*).	"(123A)" matches "123A". "408(12)+" matches "40812" and "408121212", but not "408".
\N	Matches the preceding strings in	"(string)\1" matches a string containing

Characters	Meaning	Examples
	parentheses, with the *Nth* string repeated once.	"stringstring". "(string1)(string2)\2" matches a string containing "string1string2string2". "(string1)(string2)\1\2" matches a string containing " string1string2string1string2".
[ ]	Matches a single character in the brackets.	"[16A]" matches a string containing 1, 6, or A; "[1-36A]" matches a string containing 1, 2, 3, 6, or A (- is a hyphen). To match the character "]", put it immediately after "[", for example, []abc]. There is no such limit on "[".
[^]	Matches a single character that is not in the brackets.	"[^16A]" matches a string that contains one or more characters except for 1, 6, or A, such as "abc". A match can also contain 1, 6, or A (such as "m16"), but it cannot contain these three characters only (such as 1, 16, or 16A).
{n}	Matches the preceding character *n* times. The number *n* must be a nonnegative integer.	"o{2}" matches "food", but not "Bob".
{n,}	Matches the preceding character *n* times or more. The number *n* must be a nonnegative integer.	"o{2,}" matches "foooood", but not "Bob".
{n,m}	Matches the preceding character *n* to *m* times or more. The numbers *n* and *m* must be nonnegative integers and *n* cannot be greater than *m*.	" o{1,3}" matches "fod", "food", and "foooood", but not "fd".
\<	Matches a string that starts with the pattern following \<. A string that contains the pattern is also a match if the characters preceding the pattern are not digits, letters, or underscores.	"\<do" matches "domain" and "doa".
\>	Matches a string that ends with the pattern preceding \>. A string that contains the pattern is also a match if the characters following the pattern are not digits, letters, or underscores.	"do\>" matches "undo" and "cdo".
\b	Matches a word that starts with the pattern following \b or ends with the pattern preceding \b.	"er\b" matches "never", but not "verb" or "erase". "\ber" matches "erase", but not "verb" or "never".
\B	Matches a word that contains the pattern but does not start or end with the pattern.	"er\B" matches "verb", but not "never" or "erase".
\w	Same as [A-Za-z0-9_], matches a digit, letter, or underscore.	"v\w" matches "vlan" and "service".
\W	Same as [^A-Za-z0-9_], matches a character that is not a digit, letter, or underscore.	"\Wa" matches "-a", but not "2a" or "ba".
\	Escape character. If a special character listed in this table follows \, the specific meaning of the character is removed.	"\\" matches a string containing "\", "\^" matches a string containing "^", and "\\b" matches a string containing "\b".

Examples

Configure a CLI-defined policy to monitor Syslog messages for level 3 to level 0 messages that contain the **down** string. Enable the policy to execute when five log matches are found within 6 seconds.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] event syslog priority 3 msg down occurs 5 period 6
```

event track

Use **event track** to configure a track event for a CLI-defined monitor policy.

Use **undo event** to delete the event in a CLI-defined monitor policy.

Syntax

event track *track-list* **state** { **negative** | **positive** } [**suppress-time** *suppress-time*]

undo event

Default

A CLI-defined policy does not contain a track event.

Views

CLI-defined policy view

Predefined user roles

network-admin

Parameters

track-list: Specifies a space-separated list of up to 16 track items. Each item specifies a track entry number or a range of track entry numbers in the form of *track-entry-number* **to** *track-entry-number*. The value range for the *track-entry-number* argument is 1 to 1024.

state { **negative** | **positive** }: Monitors state change of the track entries.

- **negative**: Triggers the policy when the states of the track entries change from Positive to Negative.
- **positive**: Triggers the policy when the states of the track entries change from Negative to Positive.

suppress-time *suppress-time*: Sets a suppress time in the range of 1 to 4294967295, in seconds. The default value is 0.

Usage guidelines

Use track event monitor policies to monitor state change of track entries. If you specify one track entry for a policy, EAA triggers the policy when the state of the track entry changes from Positive to Negative or from Negative to Positive. If you specify multiple track entries for a policy, EAA triggers the policy only when the state of all the track entries changes from Positive to Negative or Negative to Positive.

If you set a suppress time for a track event monitor policy, the timer starts when the policy is triggered. The system does not process the messages that report the track entry positive-to-negative or negative-to-positive state change until the timer times out.

You can configure only one event entry for a monitor policy. If the monitor policy already contains an event entry, the new event entry replaces the old event entry.

Examples

Create CLI-defined monitor policy **test**. Configure a track event for the policy that occurs when the states of track entry 1 to track entry 8 change from Positive to Negative. Set the suppress time to 180 seconds for the policy.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] event track 1 to 8 state negative suppress-time 180
```

rtm cli-policy

Use **rtm cli-policy** to create a CLI-defined EAA monitor policy and enter its view, or enter the view of an existing CLI-defined EAA monitor policy.

Use **undo rtm cli-policy** to delete a CLI-defined monitor policy.

Syntax

rtm cli-policy *policy-name*

undo rtm cli-policy *policy-name*

Default

No CLI-defined monitor policies exist.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies the name of a CLI-defined monitor policy, a case-sensitive string of 1 to 63 characters.

Usage guidelines

You must create a CLI-defined monitor policy before you can use the CLI to configure settings in the policy.

For a CLI-defined monitor policy to take effect, you must execute the **commit** command after you complete configuring the policy.

You can execute this command multiple times to create multiple CLI-defined monitor policies. Make sure the CLI-defined monitor policies that are executed at the same time do not have conflicting actions. If the actions conflict, the system executes the actions randomly.

You can assign the same name to a CLI-defined policy and a Tcl-defined policy.

Examples

Create a CLI-defined policy and enter its view.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
```

Related commands

commit

rtm environment

Use **rtm environment** to configure an EAA environment variable.

Use **undo rtm environment** to delete a user-defined EAA environment variable.

Syntax

rtm environment *var-name var-value*

undo rtm environment *var-name*

Default

No user-defined EAA environment variables exist.

The system provides the variables in Table 8. You cannot create, delete, or modify these system-defined variables.

Table 8 System-defined EAA environment variables by event type

Event	Variable name and description
Any event	_event_id: Event ID _event_type: Event type _event_type_string: Event type description _event_time: Time when the event occurs _event_severity: Severity level of an event
CLI	_cmd: Commands that are matched
Syslog	_syslog_pattern: Log message content
Hotplug	_slot: ID of the member device that joins or leaves the IRF fabric
Interface	_ifname: Interface name
SNMP	_oid: OID of the MIB variable where an SNMP operation is performed _oid_value: Value of the MIB variable
SNMP-Notification	_oid: OID that is included in the SNMP notification.
Process	_process_name: Process name

Views

System view

Predefined user roles

network-admin

Parameters

var-name: Specifies a user-defined EAA environment variable by its name, a case-sensitive string of 1 to 63 characters. The name can contain digits, letters, and the underscore sign (_), but its leading character cannot be the underscore sign.

var-value: Specifies the variable value.

Usage guidelines

When you define an action, you can enter a variable name with a leading dollar sign (**$***variable_name*) instead of entering a value for an argument. EAA will replace the variable name with the variable value when it performs the action.

For an action argument, you can specify a list of variable names in the form of **$***variable_name1***$***variable_name2...***$***variable_nameN.*

Examples

Create an environment variable: set its name to **if** and set its value to **interface**.

```
<Sysname> system-view
```

```
[Sysname] rtm environment if interface
```

rtm event syslog buffer-size

Use **rtm event syslog buffer-size** to set the size for the EAA-monitored log buffer.

Use **undo rtm event syslog buffer-size** to restore the default.

Syntax

rtm event syslog buffer-size *buffer-size*

undo rtm event syslog buffer-size

Default

The size of the EAA-monitored log buffer is 50000.

Views

System view

Predefined user roles

network-admin

Parameters

buffer-size: Specifies the size for the EAA-monitored log buffer, in the range of 1 to 500000.

Usage guidelines

After you execute a Syslog event monitor policy, the system saves a copy of the logs to the EAA-monitored log buffer. When the logs in the buffer match the Syslog event, EAA executes the monitor policy actions.

Typically, the default EAA-monitored log buffer size is sufficient. However, when a feature malfunctions or the user enables multiple debugging functions, a large number of logs are generated. Some logs might be discarded before the matching is performed. You can set the EAA-monitored log buffer to a large size based on the memory usage.

Examples

Set the size of the EAA-monitored log buffer to 1000.

```
<Sysname> system-view
[Sysname] rtm event syslog buffer-size 1000
```

Related commands

event syslog

rtm scheduler suspend

Use **rtm scheduler suspend** to suspend all monitor policies, including CLI monitor policies and Tcl monitor policies.

Use **undo rtm scheduler suspend** to resume monitor policies.

Syntax

rtm scheduler suspend

undo rtm scheduler suspend

Views

System view

Predefined user roles

network-admin

Usage guidelines

You need to suspend the monitor policies under the following circumstances:

- The monitor policies are triggered frequently, affecting the system services and performance.
- The Tcl script of a policy needs to be revised.

After you execute this command, EAA will not execute the policies even if the trigger conditions are met.

This command does not suspend a running monitor policy until all its actions are executed.

Examples

Suspend monitor policies.

```
<Sysname> system-view
[Sysname] rtm scheduler suspend
```

rtm tcl-policy

Use **rtm tcl-policy** to create a Tcl-defined policy and bind it to a Tcl script file.

Use **undo rtm tcl-policy** to delete a Tcl policy.

Syntax

rtm tcl-policy *policy-name tcl-filename*

undo rtm tcl-policy *policy-name*

Default

No Tcl policies exist.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a policy name, a case-sensitive string of 1 to 63 characters.

tcl-filename: Specifies a .tcl script file name. The file name is case sensitive. You must ensure that the file is available on a storage medium of the device.

Usage guidelines

When you use this command to create a Tcl-defined policy, follow these guidelines:

Make sure the script file is saved on all IRF member devices. This practice ensures that the policy can run correctly after a master/subordinate switchover occurs or the member device where the script file resides leaves the IRF.

This command both creates and enables the specified Tcl-defined monitor policy. To revise the Tcl script of a Tcl-defined policy, you must suspend all monitor policies first, and then resume the policies after you finish revising the script. The system cannot execute a Tcl-defined policy if you edit its Tcl script without suspending all monitor policies.

To bind a Tcl-defined policy to a different Tcl script file:

1. Execute the **undo rtm tcl-policy** command to delete the Tcl policy.

2. Create the Tcl policy again, and then bind it to the new Tcl script file.

You can assign the same policy name to a CLI-defined policy and a Tcl-defined policy. However, you cannot assign the same name to policies that are the same type.

Examples

Create a Tcl policy and bind it to a Tcl script file.

```
<Sysname> system-view
[Sysname] rtm tcl-policy test test.tcl
```

running-time

Use **running-time** to configure the action runtime of a CLI-defined policy.

Use **undo running-time** to restore the default.

Syntax

running-time *time*

undo running-time

Default

The action runtime of a CLI-defined policy is 20 seconds.

Views

CLI-defined policy view

Predefined user roles

network-admin

Parameters

time: Specifies the action runtime in the range of 0 to 31536000 seconds. If you specify 0, the policy runs its actions forever once the policy is triggered.

Usage guidelines

The action runtime limits the amount of time that the monitor policy runs its actions from the time it is triggered. When the runtime is reached, the system stops executing the actions even if the execution is not finished.

This setting prevents an incorrectly defined policy from running its actions permanently to occupy resources.

Examples

Set the action runtime to **60** seconds for CLI-defined policy **test**.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] running-time 60
```

user-role

Use **user-role** to assign a user role to a CLI-defined policy.

Use **undo user-role** to remove a user role from a CLI-defined policy.

Syntax

user-role *role-name*

undo user-role *role-name*

Default

A monitor policy contains user roles that its creator had at the time of policy creation.

Views

CLI-defined policy view

Predefined user roles

network-admin

Parameters

role-name: Specifies a user role by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

For EAA to execute an action in a monitor policy, you must assign the policy the user role that has access to the action-specific commands and resources. If EAA lacks access to an action-specific command or resource, EAA does not perform the action and all the subsequent actions.

For example, a monitor policy has four actions numbered from 1 to 4. The policy has user roles that are required for performing actions 1, 3, and 4, but it does not have the user role required for performing action 2. When the policy is triggered, EAA executes only action 1.

A monitor policy supports a maximum of 64 valid user roles. User roles added after this limit is reached do not take effect.

An EAA policy cannot have both the **security-audit** user role and any other user roles. Any previously assigned user roles are automatically removed when you assign the **security-audit** user role to the policy. The previously assigned **security-audit** user role is automatically removed when you assign any other user roles to the policy.

Examples

Assign user roles to a CLI-defined policy.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] user-role network-admin
[Sysname-rtm-test] user-role admin
```

Contents

Process monitoring and maintenance commands

The **display memory**, **display process**, **display process cpu**, **monitor process** and **monitor thread** commands display information about both user processes and kernel threads. In these commands, "process" refers to both user processes and kernel threads.

display exception context

Use **display exception context** to display context information for process exceptions.

Syntax

display exception context [**count** *value*] [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

Parameters

count *value*: Specifies the number of context information entries, in the range of 1 to 20. The default value is 1.

slot *slot-number*: Specifies an IRF member device by its ID. If you do not specify this option, the command displays context information for process exceptions on the IRF master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

The system generates a context information entry for each process exception. A context information entry includes the process ID, the crash time, the core dump file directory, stack information, and register information.

Examples

Display the exception context information on the x86-based 32-bit terminal.

```
<Sysname> display exception context
Index 1 of 1
-----------------------------
Crashed PID: 120 (routed)
Crash signal: SIGBUS
Crash time: Tue Apr  9 17:14:30 2013
Core file path:
flash:/core/node0_routed_120_7_20130409-171430_1365527670.core
#0  0xb7caba4a
#1  0x0804cb79
#2  0xb7cd77c4
#3  0x08049f45
Backtrace stopped.
                          Registers' content
```

```
  eax:0xfffffffc   ebx:0x00000003   ecx:0xbfe244ec   edx:0x0000000a
  esp:0xbfe244b8   ebp:0xbfe244c8   esi:0xffffffff   edi:0xbfe24674
  eip:0xb7caba4a eflag:0x00000292    cs:0x00000073    ss:0x0000007b
   ds:0x0000007b    es:0x0000007b    fs:0x00000000    gs:0x00000033
```

Display the exception context information on the x86-based 64-bit terminal.

```
<Sysname> display exception context
Index 1 of 1
------------------------------
Crashed PID: 121 (routed)
Crash signal: SIGBUS
Crash time: Sun Mar 31 11:12:21 2013
Core file path:
flash:/core/node0_routed_121_7_20130331-111221_1364728341.core
#0  0x00007fae7dbad20c
#1  0x00000000004059fa
#2  0x00007fae7dbd96c0
#3  0x0000000000402b29
Backtrace stopped.
                         Registers' content
       rax:0xfffffffffffffffc       rbx:0x00007fff88a5dd10
       rcx:0xffffffffffffffff       rdx:0x000000000000000a
       rsi:0x00007fff88a5dd10       rdi:0x0000000000000003
       rbp:0x00007fff88a5dcf0       rsp:0x00007fff88a5dcf0
        r8:0x00007fae7ea587e0        r9:0x0000000000000079
       r10:0xffffffffffffffff       r11:0x0000000000000246
       r12:0x0000000000405b18       r13:0x00007fff88a5ff7a
       r14:0x00007fff88a5de30       r15:0x0000000000000000
       rip:0x00007fae7dbad20c      flag:0x0000000000000246
        cs:0x0000000000000033        ss:0x000000000000002b
        ds:0x0000000000000000        es:0x0000000000000000
        fs:0x0000000000000000        gs:0x0000000000000000
   fs_base:0x00007fae80a5d6a0   gs_base:0x0000000000000000
   orig_ax:0x00000000000000e8
```

Display the exception context information on the PowerPC-based 32-bit terminal.

```
<Sysname> display exception context
Index 1 of 1
------------------------------
Crashed PID: 133 (routed)
Crash signal: SIGBUS
Crash time: Wed Apr 10 15:47:49 2013
Core file path:
flash:/core/node0_routed_133_7_20130410-154749_1365608869.core
#0  0x184720bc
#1  0x10006b4c
Backtrace stopped.
                         Registers' content
grp00: 0x000000ee 0x7ffd6ad0 0x1800f440 0x00000004
grp04: 0x7ffd6af8 0x0000000a 0xffffffff 0x184720bc
```

```
grp08: 0x0002d200 0x00000003 0x00000001 0x1847209c
grp12: 0x10006b4c 0x10020534 0xd6744100 0x00000000
grp16: 0x00000000 0xa0203ff0 0xa028b12c 0xa028b13c
grp20: 0xa028b148 0xa028b168 0xa028b178 0xa028b190
grp24: 0xa028b1a8 0xa028b1b8 0x00000000 0x7ffd6c08
grp28: 0x10006cac 0x7ffd6f92 0x184c1b84 0x7ffd6ae0

  nip:0x184720bc    lr:0x10006b4c    cr:0x38000022   ctr:0x1847209c
  msr:0x0002db00   xer:0x00000000   ret:0xfffffffc dsisr:0x08000000
  gr3:0x00000003    mq:0x00000000  trap:0x00000c00   dar:0x1833114c
```

Display the exception context information on the PowerPC-based 64-bit terminal.

```
<Sysname> display exception context
Index 1 of 1
------------------------------
Crashed PID: 172 (routed)
Crash signal: SIGBUS
Crash time: Sat Sep 15 16:53:16 2007
Core file path:
flash:/core/node1_routed_172_7_20070915-165316_1189875196.core
#0  0x00000fff803c66b4
#1  0x0000000010009b94
#2  0x00000fff80401814
Backtrace stopped.
                         Registers' content
     grp00: 0x00000000000000ee 0x00000fffffd04840
     grp02: 0x00000fff80425c28 0x0000000000000004
     grp04: 0x00000fffffd048c0 0x000000000000000a
     grp06: 0xffffffffffffffff 0x00000fff803c66b4
     grp08: 0x000000008002d000 0x0000000000000000
     grp10: 0x0000000000000000 0x0000000000000000
     grp12: 0x0000000000000000 0x00000fff80a096b0
     grp14: 0x000000007b964c00 0x000000007b7d0000
     grp16: 0x0000000000000001 0x000000000000000b
     grp18: 0x0000000000000031 0x0000000000a205b8
     grp20: 0x0000000000a20677 0x0000000000000000
     grp22: 0x000000007bb91014 0x0000000000000000
     grp24: 0xc0000000005ae1c8 0x0000000000000000
     grp26: 0xc0000001f00bff20 0xc0000001f00b0000
     grp28: 0x00000fffffd04a30 0x0000000001001aed8
     grp30: 0x00000fffffd04fae 0x00000fffffd04840

       nip:0x00000fff803c66b4        lr:0x0000000010009b94
        cr:0x0000000058000482       ctr:0x00000fff803c66ac
       msr:0x000000008002d000       xer:0x0000000000000000
       ret:0xfffffffffffffffc     dsisr:0x0000000000000000
       gr3:0x0000000000000003     softe:0x0000000000000001
      trap:0x0000000000000c00       dar:0x00000fff8059d14c
```

Display the exception context information on the MIPS-based 32-bit terminal.

```
<Sysname> display exception context
Index 1 of 1
------------------------------
Crashed PID: 182 (routed)
Crash signal: SIGBUS
Crash time: Sun Jan  2 08:11:38 2013
Core file path:
flash:/core/node4_routed_182_10_20130102-081138_1293955898.core
#0  0x2af2faf4
#1  0x00406d8c
Backtrace stopped.
                        Registers' content
 zero:0x00000000   at:0x1000dc00   v0:0x00000004   v1:0x00000003
   a0:0x00000003   a1:0x7fd267e8   a2:0x0000000a   a3:0x00000001
   t0:0x00000000   t1:0xcf08fa14   t2:0x80230510   t3:0xfffffff8
   t4:0x69766520   t5:0x00000000   t6:0x63cc6000   t7:0x44617461
   s0:0x7fd26f81   s1:0x00401948   s2:0x7fd268f8   s3:0x803e1db0
   s4:0x803e1da0   s5:0x803e1d88   s6:0x803e1d70   s7:0x803e1d60
   t8:0x00000008   t9:0x2af2fae0   k0:0x00000000   k1:0x00000000
   gp:0x2af9a3a0   sp:0x7fd267c0   s8:0x7fd267c0   ra:0x00406d8c
   sr:0x0000dc13   lo:0xef9db265   hi:0x0000003f  bad:0x2add2010
cause:0x00800020   pc:0x2af2faf4
```

Display the exception context information on the MIPS-based 64-bit terminal.

```
<Sysname> display exception context
Index 1 of 1
------------------------------
Crashed PID: 270 (routed)
Crash signal: SIGBUS
Crash time: Wed Mar 27 12:39:12 2013
Core file path:
flash:/core/node16_routed_270_10_20130327-123912_1364387952.core
#0  0x0000005555a3bcb4
#1  0x0000000120006c1c
Backtrace stopped.
                        Registers' content
      zero:0x0000000000000000        at:0x0000000000000014
        v0:0x0000000000000004        v1:0x0000000000000003
        a0:0x0000000000000003        a1:0x000000ffff899d90
        a2:0x000000000000000a        a3:0x0000000000000001
        a4:0x0000005555a9b4e0        a5:0x0000000000000000
        a6:0xffffffff8021349c        a7:0x20696e206368616e
        t0:0x0000000000000000        t1:0xffffffff80105068
        t2:0xffffffff80213890        t3:0x0000000000000008
        s0:0x0000005555a99c40        s1:0x000000ffff89af5f
        s2:0x0000000120007320        s3:0x0000005555a5f470
        s4:0x000000ffff899f80        s5:0xffffffff803cc6c0
        s6:0xffffffff803cc6a8        s7:0xffffffff803cc690
        t8:0x0000000000000002        t9:0x0000005555a3bc98
```

```
      k0:0x0000000000000000        k1:0x0000000000000000
      gp:0x0000000120020460        sp:0x000000ffff899d70
      s8:0x000000ffff899d80        ra:0x0000000120006c1c
      sr:0x000000000400fff3        lo:0xdf3b645a1cac08c9
      hi:0x000000000000007f       bad:0x000000555589ba84
   cause:0x0000000000800020        pc:0x0000005555a3bcb4
```

Table 1 Command output

Filed	Description
Crashed PID	ID of the crashed process.
Crash signal	Signals that led to the crash: • **SIGABRT**—Abort. • **SIGBUS**—Bus error. • **SIGFPE**—Erroneous arithmetic operation. • **SIGILL**—Illegal hardware instructions. • **SIGQUIT**—Quit signal sent by the controlling terminal. • **SIGSEGV**—Invalid memory access. • **SIGSYS**—Invalid system call. • **SIGTRAP**—Trap message. • **SIGXCPU**—CPU usage limit exceeded. • **SIGXFSZ**—File size limit exceeded. • **SIGUNKNOW**—Unknown reason.
Crash time	Time when the crash occurred.
Core file path	Directory where the core dump file is saved.
Backtrace stopped	All stack information has been displayed.

Related commands

`reset exception context`

display exception filepath

Use **`display exception filepath`** to display the core dump file directory.

Syntax

`display exception filepath` [**`slot`** *`slot-number`* [**`cpu`** *`cpu-number`*]]

Views

Any view

Predefined user roles

network-admin

Parameters

`slot` *`slot-number`*: Specifies an IRF member device by its ID. If you do not specify this option, the command displays the core dump file directory on the IRF master device.

`cpu` *`cpu-number`*: Specifies a CPU by its number.

Examples

Display the core dump file directory on the specified slot.

```
<Sysname> display exception filepath slot 1
The exception filepath on slot 1 is flash:.
```

display kernel deadloop

Use **display kernel deadloop** to display kernel thread deadloop information.

Syntax

display kernel deadloop *show-number* [*offset*] [**verbose**] [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

Parameters

show-number: Specifies the number of deadloops to display, in the range of 1 to 20.

offset: Specifies the offset between the starting deadloop and the most recent deadloop, in the range of 0 to 19. The default value is 0.

verbose: Displays detailed information. If you do not specify this keyword, the command displays brief information.

slot *slot-number*: Specifies an IRF member device by its ID. If you do not specify this option, the command displays kernel thread deadloop information for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Examples

Display brief information about the most recent kernel thread deadloop.

```
<Sysname> display kernel deadloop 1
----------------- Deadloop record 1 -----------------
Description          : BUG: soft lockup - CPU#0 stuck for 61! [comsh: 16306]
Recorded at          : 2013-05-01  11:16:00.823018
Occurred at          : 2013-05-01  11:16:00.823018
Instruction address  : 0x4004158c
Thread               : comsh (TID: 16306)
Context              : thread context
Slot                 : 1
Cpu                  : 0
VCPU ID              : 0
Kernel module info   : module name (mrpnc) module address (0xe332a000)
```

Display detailed information about the most recent kernel thread deadloop.

```
<Sysname> display kernel deadloop 1 verbose
----------------- Deadloop record 1 -----------------
Description          : BUG: soft lockup - CPU#0 stuck for 61! [comsh: 16306]
Recorded at          : 2013-05-01  11:16:00.823018
Occurred at          : 2013-05-01  11:16:00.823018
Instruction address  : 0x4004158c
Thread               : comsh (TID: 16306)
Context              : thread context
```

```
Slot                : 1
Cpu                 : 0
VCPU ID             : 0
Kernel module info  : module name (mrpnc) module address (0xe332a000)

Last 5 thread switches : migration/0 (11:16:00.823018)-->
                         swapper (11:16:00.833018)-->
                         kthreadd (11:16:00.833518)-->
                         swapper (11:16:00.833550)-->
                         disk (11:16:00.833560)

Register content:
Reg:       r0, Val = 0x00000000 ; Reg:       r1, Val = 0xe2be5ea0 ;
Reg:       r2, Val = 0x00000000 ; Reg:       r3, Val = 0x77777777 ;
Reg:       r4, Val = 0x00000000 ; Reg:       r5, Val = 0x00001492 ;
Reg:       r6, Val = 0x00000000 ; Reg:       r7, Val = 0x0000ffff ;
Reg:       r8, Val = 0x77777777 ; Reg:       r9, Val = 0x00000000 ;
Reg:      r10, Val = 0x00000001 ; Reg:      r11, Val = 0x0000002c ;
Reg:      r12, Val = 0x057d9484 ; Reg:      r13, Val = 0x00000000 ;
Reg:      r14, Val = 0x00000000 ; Reg:      r15, Val = 0x02000000 ;
Reg:      r16, Val = 0xe2be5f00 ; Reg:      r17, Val = 0x00000000 ;
Reg:      r18, Val = 0x00000000 ; Reg:      r19, Val = 0x00000000 ;
Reg:      r20, Val = 0x024c10f8 ; Reg:      r21, Val = 0x057d9244 ;
Reg:      r22, Val = 0x00002000 ; Reg:      r23, Val = 0x0000002c ;
Reg:      r24, Val = 0x00000002 ; Reg:      r25, Val = 0x24000024 ;
Reg:      r26, Val = 0x00000000 ; Reg:      r27, Val = 0x057d9484 ;
Reg:      r28, Val = 0x0000002c ; Reg:      r29, Val = 0x00000000 ;
Reg:      r30, Val = 0x0000002c ; Reg:      r31, Val = 0x00000000 ;
Reg:       cr, Val = 0x84000028 ; Reg:      nip, Val = 0x057d9550 ;
Reg:      xer, Val = 0x00000000 ; Reg:       lr, Val = 0x0186eff0 ;
Reg:      ctr, Val = 0x682f7344 ; Reg:      msr, Val = 0x00784b5c ;
Reg:     trap, Val = 0x0000b030 ; Reg:      dar, Val = 0x77777777 ;
Reg:    dsisr, Val = 0x40000000 ; Reg:   result, Val = 0x00020300 ;

Dump stack (total 1024 bytes, 16 bytes/line):
0xe2be5ea0: 02 be 5e c0 24 00 00 24 00 00 00 00 05 7d 94 84
0xe2be5eb0: 00 00 00 04 00 00 00 00 00 00 00 28 05 8d 34 c4
0xe2be5ec0: 02 be 60 a0 01 86 ef f0 00 00 00 00 00 00 00 00
0xe2be5ed0: 02 04 05 b4 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5ee0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5ef0: 95 47 73 35 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f00: a0 e1 64 21 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f10: 00 00 00 00 00 00 00 00 00 00 00 00 01 e9 00 00
0xe2be5f20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f30: 00 00 00 00 00 00 00 00 02 be 66 c0 02 be 66 d0
0xe2be5f40: 02 be 61 e0 00 00 00 02 00 00 00 00 02 44 b3 a4
0xe2be5f50: 02 be 5f 90 00 00 00 08 02 be 5f e0 00 00 00 08
0xe2be5f60: 02 be 5f 80 00 ac 1b 14 00 00 00 00 00 00 00 00
```

```
0xe2be5f70: 05 b4 5f 90 02 be 5f e0 00 00 00 30 02 be 5f e0
0xe2be5f80: 02 be 5f c0 00 ac 1b f4 00 00 00 00 02 45 00 00
0xe2be5f90: 00 03 00 00 00 00 00 00 02 be 5f e0 00 00 00 30
0xe2be5fa0: 02 be 5f c0 00 ac 1b 14 61 f1 2e ae 02 45 00 00
0xe2be5fb0: 02 44 b3 74 02 be 5f d0 00 00 00 30 02 be 5f e0
0xe2be5fc0: 02 be 60 60 01 74 ff f8 00 00 00 00 00 00 08 00
0xe2be5fd0: 02 be 5f f0 00 e8 93 7e 02 be 5f f8 02 be 5f fc
0xe2be5fe0: 00 00 00 00 00 00 00 00 00 00 00 00 02 be 60 18
0xe2be5ff0: 02 be 60 10 00 e9 65 98 00 00 00 58 00 00 2a 4f
0xe2be6000: 02 be 60 10 00 00 00 00 00 00 00 00 02 be 60 68
0xe2be6010: 02 be 60 40 00 e8 c6 a0 00 00 11 17 00 00 00 00
0xe2be6020: 02 be 60 40 00 00 00 00 00 00 00 00 02 be 60 98
0xe2be6030: 02 27 00 00 00 00 00 00 00 00 00 00 02 be 60 68
0xe2be6040: 02 be 60 60 00 00 00 01 00 00 b0 30 02 be 60 98
0xe2be6050: 00 00 00 04 02 21 00 00 00 00 00 00 01 e9 00 00
0xe2be6060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be6070: 00 00 00 00 00 00 00 00 02 be 66 c0 02 be 66 d0
0xe2be6080: 02 be 61 e0 00 00 00 02 00 00 00 00 02 be 61 70
0xe2be6090: 00 00 00 00 02 21 00 00 05 8d 34 c4 05 7d 92 44

Call trace:
Function Address = 0x8012a4b4
Function Address = 0x8017989c
Function Address = 0x80179b30
Function Address = 0x80127438
Function Address = 0x8012d734
Function Address = 0x80100a00
Function Address = 0xe0071004
Function Address = 0x8016ce0c
Function Address = 0x801223a0

Instruction dump:
41a2fe9c 812300ec 800200ec 7f890000 409efe8c 80010014 540b07b9 40a2fe80
4bfffe6c 80780290 7f64db78 4804ea35 <807f002c> 38800000 38a00080 3863000c
```

Table 2 Command output

Field	Description
Description	Description for the kernel thread deadloop, including the CPU number, thread running time, thread name, and thread number.
Recorded at	Time when the kernel thread deadloop was recorded, with microsecond precision.
Occurred at	Time when the kernel thread deadloop occurred, with microsecond precision.
Instruction address	Instruction address for the kernel thread deadloop.
Thread	Name and number of the kernel thread deadloop.
Context	Context for the kernel thread deadloop.
Cpu	Number of the CPU where the kernel thread ran.

Field	Description
VCPU ID	Number of the CPU core where the kernel thread ran.
Kernel module info	Information about kernel modules that had been loaded when the kernel thread deadloop was detected, including: • **Module name**—Kernel module name. • **Module address**—Memory address of the module.
Last 5 thread switches	Last five kernel thread switches on the CPU before the kernel thread deadloop was detected, including kernel thread name and kernel thread switching time with microsecond precision.
Register content	Register information: • **Reg**—Name of a register. • **Val**—Value saved in a register.
Dump stack	Stack information.
Call trace	Function call stack information, which shows the instruction address of a called function at each level.
Instruction dump	Instruction code when the kernel thread deadloop was detected. **ffffffff** indicates an illegitimate instruction code.
No information to display	No kernel thread deadloop information.

Related commands

reset kernel deadloop

display kernel deadloop configuration

Use **display kernel deadloop configuration** to display kernel thread deadloop detection configuration.

Syntax

display kernel deadloop configuration [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its ID. If you do not specify this option, the command displays kernel thread deadloop detection configuration for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Examples

Display kernel thread deadloop detection configuration.

```
<Sysname> display kernel deadloop configuration
Thread dead loop detection: Enabled
Dead loop timer (in seconds): 20
Dead loop core list: 0-1
Dead loop action: Record-only
Threads excluded from monitoring: 1
```

```
  TID:     15   Name: co0
```

Table 3 Command output

Field	Description
Dead loop timer (in seconds): *n*	Time interval (in seconds) to identify a kernel thread deadloop. A kernel thread deadloop occurs if a kernel thread runs more than *n* seconds.
Dead loop core list	CPU cores for which kernel thread deadloop detection is performed.
Dead loop action	Action to be taken in response to a kernel thread deadloop: • **Reboot**—Logs the event and reboots the hardware. • **Record-only**—Logs the event.
Threads excluded from monitoring	Kernel threads excluded from kernel thread deadloop detection. This field appears only if the **monitor kernel deadloop exclude-thread** command is configured.
Name	Kernel thread name.
TID	Kernel thread number.
No thread is excluded from monitoring	All kernel threads are monitored by kernel thread deadloop detection.

display kernel exception

Use **display kernel exception** to display kernel thread exception information.

Syntax

display kernel exception *show-number* [*offset*] [**verbose**] [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

Parameters

show-number: Specifies the number of kernel exceptions to display, in the range of 1 to 20.

offset: Specifies the offset between the starting exception and the most recent exception, in the range of 0 to 19. The default value is 0.

verbose: Displays detailed information. If you do not specify this keyword, the command displays brief information.

slot *slot-number*: Specifies an IRF member device by its ID. If you do not specify this option, the command displays kernel thread exception information for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

If an exception occurs to a running kernel thread, the system automatically records the exception information.

Examples

Display brief information about the most recent kernel thread exception.

```
<Sysname> display kernel exception 1
----------------- Exception record 1 -----------------
Description          : Oops[#0]
Recorded at          : 2013-05-01  11:16:00.823018
Occurred at          : 2013-05-01  11:16:00.823018
Instruction address  : 0x4004158c
Thread               : comsh (TID: 16306)
Context              : thread context
Slot                 : 1
Cpu                  : 0
VCPU ID              : 0
Kernel module info   : module name (mrpnc) module address (0xe332a000)
                       module name (disk) module address (0xe00bd000)
```

Display detailed information about the most recent kernel thread exception.

```
<Sysname> display kernel exception 1 verbose
----------------- Exception record 1 -----------------
Description          : Oops[#0]
Recorded at          : 2013-05-01  11:16:00.823018
Occurred at          : 2013-05-01  11:16:00.823018
Instruction address  : 0x4004158c
Thread               : comsh (TID: 16306)
Context              : thread context
Slot                 : 1
Cpu                  : 0
VCPU ID              : 0
Kernel module info   : module name (mrpnc) module address (0xe332a000)
                       module name (12500) module address (0xe00bd000)

Last 5 thread switches : migration/0 (11:16:00.823018)-->
                         swapper (11:16:00.833018)-->
                         kthreadd (11:16:00.833518)-->
                         swapper (11:16:00.833550)-->
                         disk (11:16:00.833560)

Register content:
Reg:       r0, Val = 0x00000000 ; Reg:       r1, Val = 0xe2be5ea0 ;
Reg:       r2, Val = 0x00000000 ; Reg:       r3, Val = 0x77777777 ;
Reg:       r4, Val = 0x00000000 ; Reg:       r5, Val = 0x00001492 ;
Reg:       r6, Val = 0x00000000 ; Reg:       r7, Val = 0x0000ffff ;
Reg:       r8, Val = 0x77777777 ; Reg:       r9, Val = 0x00000000 ;
Reg:      r10, Val = 0x00000001 ; Reg:      r11, Val = 0x0000002c ;
Reg:      r12, Val = 0x057d9484 ; Reg:      r13, Val = 0x00000000 ;
Reg:      r14, Val = 0x00000000 ; Reg:      r15, Val = 0x02000000 ;
Reg:      r16, Val = 0xe2be5f00 ; Reg:      r17, Val = 0x00000000 ;
Reg:      r18, Val = 0x00000000 ; Reg:      r19, Val = 0x00000000 ;
Reg:      r20, Val = 0x024c10f8 ; Reg:      r21, Val = 0x057d9244 ;
Reg:      r22, Val = 0x00002000 ; Reg:      r23, Val = 0x0000002c ;
Reg:      r24, Val = 0x00000002 ; Reg:      r25, Val = 0x24000024 ;
```

```
Reg:      r26, Val = 0x00000000 ; Reg:      r27, Val = 0x057d9484 ;
Reg:      r28, Val = 0x0000002c ; Reg:      r29, Val = 0x00000000 ;
Reg:      r30, Val = 0x0000002c ; Reg:      r31, Val = 0x00000000 ;
Reg:       cr, Val = 0x84000028 ; Reg:      nip, Val = 0x057d9550 ;
Reg:      xer, Val = 0x00000000 ; Reg:       lr, Val = 0x0186eff0 ;
Reg:      ctr, Val = 0x682f7344 ; Reg:      msr, Val = 0x00784b5c ;
Reg:     trap, Val = 0x0000b030 ; Reg:      dar, Val = 0x77777777 ;
Reg:    dsisr, Val = 0x40000000 ; Reg:   result, Val = 0x00020300 ;

Dump stack (total 1024 bytes, 16 bytes/line):
0xe2be5ea0: 02 be 5e c0 24 00 00 24 00 00 00 00 05 7d 94 84
0xe2be5eb0: 00 00 00 04 00 00 00 00 00 00 00 28 05 8d 34 c4
0xe2be5ec0: 02 be 60 a0 01 86 ef f0 00 00 00 00 00 00 00 00
0xe2be5ed0: 02 04 05 b4 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5ee0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5ef0: 95 47 73 35 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f00: a0 e1 64 21 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f10: 00 00 00 00 00 00 00 00 00 00 00 00 01 e9 00 00
0xe2be5f20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f30: 00 00 00 00 00 00 00 00 02 be 66 c0 02 be 66 d0
0xe2be5f40: 02 be 61 e0 00 00 00 02 00 00 00 00 02 44 b3 a4
0xe2be5f50: 02 be 5f 90 00 00 00 08 02 be 5f e0 00 00 00 08
0xe2be5f60: 02 be 5f 80 00 ac 1b 14 00 00 00 00 00 00 00 00
0xe2be5f70: 05 b4 5f 90 02 be 5f e0 00 00 00 30 02 be 5f e0
0xe2be5f80: 02 be 5f c0 00 ac 1b f4 00 00 00 00 02 45 00 00
0xe2be5f90: 00 03 00 00 00 00 00 00 02 be 5f e0 00 00 00 30
0xe2be5fa0: 02 be 5f c0 00 ac 1b 14 61 f1 2e ae 02 45 00 00
0xe2be5fb0: 02 44 b3 74 02 be 5f d0 00 00 00 30 02 be 5f e0
0xe2be5fc0: 02 be 60 60 01 74 ff f8 00 00 00 00 00 00 08 00
0xe2be5fd0: 02 be 5f f0 00 e8 93 7e 02 be 5f f8 02 be 5f fc
0xe2be5fe0: 00 00 00 00 00 00 00 00 00 00 00 00 02 be 60 18
0xe2be5ff0: 02 be 60 10 00 e9 65 98 00 00 00 58 00 00 2a 4f
0xe2be6000: 02 be 60 10 00 00 00 00 00 00 00 00 02 be 60 68
0xe2be6010: 02 be 60 40 00 e8 c6 a0 00 00 11 17 00 00 00 00
0xe2be6020: 02 be 60 40 00 00 00 00 00 00 00 00 02 be 60 98
0xe2be6030: 02 27 00 00 00 00 00 00 00 00 00 00 02 be 60 68
0xe2be6040: 02 be 60 60 00 00 00 01 00 00 b0 30 02 be 60 98
0xe2be6050: 00 00 00 04 02 21 00 00 00 00 00 00 01 e9 00 00
0xe2be6060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be6070: 00 00 00 00 00 00 00 00 02 be 66 c0 02 be 66 d0
0xe2be6080: 02 be 61 e0 00 00 00 02 00 00 00 00 02 be 61 70
0xe2be6090: 00 00 00 00 02 21 00 00 05 8d 34 c4 05 7d 92 44

Call trace:
Function Address = 0x8012a4b4
Function Address = 0x8017989c
Function Address = 0x80179b30
Function Address = 0x80127438
```

```
Function Address = 0x8012d734
Function Address = 0x80100a00
Function Address = 0xe0071004
Function Address = 0x8016ce0c
Function Address = 0x801223a0

Instruction dump:
41a2fe9c 812300ec 800200ec 7f890000 409efe8c 80010014 540b07b9 40a2fe80
4bfffe6c 80780290 7f64db78 4804ea35 <807f002c> 38800000 38a00080 3863000c
```

For more information about the command output, see Table 2.

Related commands

reset kernel exception

display kernel reboot

Use **display kernel reboot** to display reboot information for member devices.

Syntax

display kernel reboot *show-number* [*offset*] [**verbose**] [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

Parameters

show-number: Specifies the number of reboots to display, in the range of 1 to 20.

offset: Specifies the offset between the starting reboot and the most recent reboot, in the range of 0 to 19. The default value is 0.

verbose: Displays detailed information. If you do not specify this keyword, the command displays brief information.

slot *slot-number*: Specifies an IRF member device by its ID. If you do not specify this option, the command displays reboot information for the master device. Reboot information for member devices is recorded in the memory of the master device. If the master device is powered off, the reboot information is lost.

cpu *cpu-number*: Specifies a CPU by its number.

Examples

Display brief information about the most recent reboot.

```
<Sysname> display kernel reboot 1
----------------- Reboot record 1 -----------------
Recorded at          : 2013-05-01  11:16:00.823018
Occurred at          : 2013-05-01  11:16:00.823018
Reason               : 0x31
Thread               : comsh (TID: 16306)
Context              : thread context
Slot                 : 1
Target Slot          : 0
```

```
Cpu                  : 0
VCPU ID              : 0
Kernel module info   : module name (mrpnc) module address (0xe332a000)
                       module name (12500) module address (0xe00bd000)
```

Display detailed information about the most recent reboot.

```
<Sysname> display kernel reboot 1 verbose
----------------- Reboot record 1 -----------------
Recorded at          : 2013-05-01  11:16:00.823018
Occurred at          : 2013-05-01  11:16:00.823018
Reason               : 0x31
Thread               : comsh (TID: 16306)
Context              : thread context
Slot                 : 1
Target Slot          : 0
Cpu                  : 0
VCPU ID              : 0
Kernel module info   : module name (mrpnc) module address (0xe332a000)
                       module name (12500) module address (0xe00bd000)

Last 5 thread switches : migration/0 (11:16:00.823018)-->
                         swapper (11:16:00.833018)-->
                         kthreadd (11:16:00.833518)-->
                         swapper (11:16:00.833550)-->
                         disk (11:16:00.833560)

Dump stack (total 1024 bytes, 16 bytes/line):
0xe2be5ea0: 02 be 5e c0 24 00 00 24 00 00 00 00 05 7d 94 84
0xe2be5eb0: 00 00 00 04 00 00 00 00 00 00 00 28 05 8d 34 c4
0xe2be5ec0: 02 be 60 a0 01 86 ef f0 00 00 00 00 00 00 00 00
0xe2be5ed0: 02 04 05 b4 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5ee0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5ef0: 95 47 73 35 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f00: a0 e1 64 21 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f10: 00 00 00 00 00 00 00 00 00 00 00 00 01 e9 00 00
0xe2be5f20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f30: 00 00 00 00 00 00 00 00 02 be 66 c0 02 be 66 d0
0xe2be5f40: 02 be 61 e0 00 00 00 02 00 00 00 00 02 44 b3 a4
0xe2be5f50: 02 be 5f 90 00 00 00 08 02 be 5f e0 00 00 00 08
0xe2be5f60: 02 be 5f 80 00 ac 1b 14 00 00 00 00 00 00 00 00
0xe2be5f70: 05 b4 5f 90 02 be 5f e0 00 00 00 30 02 be 5f e0
0xe2be5f80: 02 be 5f c0 00 ac 1b f4 00 00 00 00 02 45 00 00
0xe2be5f90: 00 03 00 00 00 00 00 00 02 be 5f e0 00 00 00 30
0xe2be5fa0: 02 be 5f c0 00 ac 1b 14 61 f1 2e ae 02 45 00 00
0xe2be5fb0: 02 44 b3 74 02 be 5f d0 00 00 00 30 02 be 5f e0
0xe2be5fc0: 02 be 60 60 01 74 ff f8 00 00 00 00 00 00 08 00
0xe2be5fd0: 02 be 5f f0 00 e8 93 7e 02 be 5f f8 02 be 5f fc
0xe2be5fe0: 00 00 00 00 00 00 00 00 00 00 00 00 02 be 60 18
0xe2be5ff0: 02 be 60 10 00 e9 65 98 00 00 00 58 00 00 2a 4f
```

```
0xe2be6000: 02 be 60 10 00 00 00 00 00 00 00 00 02 be 60 68
0xe2be6010: 02 be 60 40 00 e8 c6 a0 00 00 11 17 00 00 00 00
0xe2be6020: 02 be 60 40 00 00 00 00 00 00 00 00 02 be 60 98
0xe2be6030: 02 27 00 00 00 00 00 00 00 00 00 00 02 be 60 68
0xe2be6040: 02 be 60 60 00 00 00 01 00 00 b0 30 02 be 60 98
0xe2be6050: 00 00 00 04 02 21 00 00 00 00 00 00 01 e9 00 00
0xe2be6060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be6070: 00 00 00 00 00 00 00 00 02 be 66 c0 02 be 66 d0
0xe2be6080: 02 be 61 e0 00 00 00 02 00 00 00 00 02 be 61 70
0xe2be6090: 00 00 00 00 02 21 00 00 05 8d 34 c4 05 7d 92 44

Call trace:
Function Address = 0x8012a4b4
Function Address = 0x8017989c
Function Address = 0x80179b30
Function Address = 0x80127438
Function Address = 0x8012d734
Function Address = 0x80100a00
Function Address = 0xe0071004
Function Address = 0x8016ce0c
Function Address = 0x801223a0
```

Table 4 Command output

Field	Description
Recorded at	Time when the reboot was recorded, with microsecond precision.
Occurred at	Time when the reboot occurred, with microsecond precision.
Reason	Reboot reason.
Thread	Name and number of the kernel thread that was running when the reboot occurred.
Context	Context where the reboot occurred.
Slot	Number of the slot that triggered the reboot.
Target Slot	Number of the rebooted slot.
Cpu	Number of the CPU that triggered the reboot.
VCPU ID	Number of the CPU core that triggered the reboot.
Kernel module info	Information about kernel modules that had been loaded when the reboot occurred, including the kernel module names and memory addresses.
Last 5 thread switches	Last five kernel thread switches that occurred on the CPU before the reboot, including the kernel thread names and kernel thread switching time points, with microsecond precision.
Dump stack	Stack information for the threads that were running when the reboot occurred.
Call trace	Function call stack information.
No information to display	No reboot information exists.

Related commands

reset kernel reboot

display kernel starvation

Use **display kernel starvation** to display kernel thread starvation information.

Syntax

display kernel starvation *show-number* [*offset*] [**verbose**] [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

Parameters

show-number: Specifies the number of thread starvations to display, in the range of 1 to 20.

offset: Specifies the offset between the starting starvation and the most recent starvation, in the range of 0 to 19. The default value is 0.

verbose: Displays detailed information. If you do not specify this keyword, the command displays brief information.

slot *slot-number*: Specifies an IRF member device by its ID. If you do not specify this option, the command displays kernel thread starvation information for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Examples

Display brief information about the most recent kernel thread starvation.

```
<Sysname> display kernel starvation 1
---------------- Starvation record 1 ----------------
Description          : INFO: task comsh: 16306 blocked for more than 10 seconds.
Recorded at          : 2013-05-01  11:16:00.823018
Occurred at          : 2013-05-01  11:16:00.823018
Instruction address  : 0x4004158c
Thread               : comsh (TID: 16306)
Context              : thread context
Slot                 : 1
Cpu                  : 0
VCPU ID              : 0
Kernel module info   : module name (mrpnc) module address (0xe332a000)
                       module name (12500) module address (0xe00bd000)
```

Display detailed information about the most recent kernel thread starvation.

```
<Sysname> display kernel starvation 1 verbose
---------------- Starvation record 1 ----------------
Description          : INFO: task comsh: 16306 blocked for more than 10 seconds.
Recorded at          : 2013-05-01  11:16:00.823018
Occurred at          : 2013-05-01  11:16:00.823018
Instruction address  : 0x4004158c
Thread               : comsh (TID: 16306)
Context              : thread context
Slot                 : 1
```

```
Cpu                  : 0
VCPU ID              : 0
Kernel module info   : module name (mrpnc) module address (0xe332a000)
                       module name (12500) module address (0xe00bd000)

Last 5 thread switches : migration/0 (11:16:00.823018)-->
                         swapper (11:16:00.833018)-->
                         kthreadd (11:16:00.833518)-->
                         swapper (11:16:00.833550)-->
                         disk (11:16:00.833560)

Register content:
Reg:       r0, Val = 0x00000000 ; Reg:       r1, Val = 0xe2be5ea0 ;
Reg:       r2, Val = 0x00000000 ; Reg:       r3, Val = 0x77777777 ;
Reg:       r4, Val = 0x00000000 ; Reg:       r5, Val = 0x00001492 ;
Reg:       r6, Val = 0x00000000 ; Reg:       r7, Val = 0x0000ffff ;
Reg:       r8, Val = 0x77777777 ; Reg:       r9, Val = 0x00000000 ;
Reg:      r10, Val = 0x00000001 ; Reg:      r11, Val = 0x0000002c ;
Reg:      r12, Val = 0x057d9484 ; Reg:      r13, Val = 0x00000000 ;
Reg:      r14, Val = 0x00000000 ; Reg:      r15, Val = 0x02000000 ;
Reg:      r16, Val = 0xe2be5f00 ; Reg:      r17, Val = 0x00000000 ;
Reg:      r18, Val = 0x00000000 ; Reg:      r19, Val = 0x00000000 ;
Reg:      r20, Val = 0x024c10f8 ; Reg:      r21, Val = 0x057d9244 ;
Reg:      r22, Val = 0x00002000 ; Reg:      r23, Val = 0x0000002c ;
Reg:      r24, Val = 0x00000002 ; Reg:      r25, Val = 0x24000024 ;
Reg:      r26, Val = 0x00000000 ; Reg:      r27, Val = 0x057d9484 ;
Reg:      r28, Val = 0x0000002c ; Reg:      r29, Val = 0x00000000 ;
Reg:      r30, Val = 0x0000002c ; Reg:      r31, Val = 0x00000000 ;
Reg:       cr, Val = 0x84000028 ; Reg:      nip, Val = 0x057d9550 ;
Reg:      xer, Val = 0x00000000 ; Reg:       lr, Val = 0x0186eff0 ;
Reg:      ctr, Val = 0x682f7344 ; Reg:      msr, Val = 0x00784b5c ;
Reg:     trap, Val = 0x0000b030 ; Reg:      dar, Val = 0x77777777 ;
Reg:    dsisr, Val = 0x40000000 ; Reg:   result, Val = 0x00020300 ;

Dump stack (total 1024 bytes, 16 bytes/line):
0xe2be5ea0: 02 be 5e c0 24 00 00 24 00 00 00 00 05 7d 94 84
0xe2be5eb0: 00 00 00 04 00 00 00 00 00 00 00 28 05 8d 34 c4
0xe2be5ec0: 02 be 60 a0 01 86 ef f0 00 00 00 00 00 00 00 00
0xe2be5ed0: 02 04 05 b4 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5ee0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5ef0: 95 47 73 35 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f00: a0 e1 64 21 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f10: 00 00 00 00 00 00 00 00 00 00 00 00 01 e9 00 00
0xe2be5f20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f30: 00 00 00 00 00 00 00 00 02 be 66 c0 02 be 66 d0
0xe2be5f40: 02 be 61 e0 00 00 00 02 00 00 00 00 02 44 b3 a4
0xe2be5f50: 02 be 5f 90 00 00 00 08 02 be 5f e0 00 00 00 08
0xe2be5f60: 02 be 5f 80 00 ac 1b 14 00 00 00 00 00 00 00 00
```

```
0xe2be5f70: 05 b4 5f 90 02 be 5f e0 00 00 00 30 02 be 5f e0
0xe2be5f80: 02 be 5f c0 00 ac 1b f4 00 00 00 00 02 45 00 00
0xe2be5f90: 00 03 00 00 00 00 00 00 02 be 5f e0 00 00 00 30
0xe2be5fa0: 02 be 5f c0 00 ac 1b 14 61 f1 2e ae 02 45 00 00
0xe2be5fb0: 02 44 b3 74 02 be 5f d0 00 00 00 30 02 be 5f e0
0xe2be5fc0: 02 be 60 60 01 74 ff f8 00 00 00 00 00 00 08 00
0xe2be5fd0: 02 be 5f f0 00 e8 93 7e 02 be 5f f8 02 be 5f fc
0xe2be5fe0: 00 00 00 00 00 00 00 00 00 00 00 00 02 be 60 18
0xe2be5ff0: 02 be 60 10 00 e9 65 98 00 00 00 58 00 00 2a 4f
0xe2be6000: 02 be 60 10 00 00 00 00 00 00 00 00 02 be 60 68
0xe2be6010: 02 be 60 40 00 e8 c6 a0 00 00 11 17 00 00 00 00
0xe2be6020: 02 be 60 40 00 00 00 00 00 00 00 00 02 be 60 98
0xe2be6030: 02 27 00 00 00 00 00 00 00 00 00 00 02 be 60 68
0xe2be6040: 02 be 60 60 00 00 00 01 00 00 b0 30 02 be 60 98
0xe2be6050: 00 00 00 04 02 21 00 00 00 00 00 00 01 e9 00 00
0xe2be6060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be6070: 00 00 00 00 00 00 00 00 02 be 66 c0 02 be 66 d0
0xe2be6080: 02 be 61 e0 00 00 00 02 00 00 00 00 02 be 61 70
0xe2be6090: 00 00 00 00 02 21 00 00 05 8d 34 c4 05 7d 92 44

Call trace:
Function Address = 0x8012a4b4
Function Address = 0x8017989c
Function Address = 0x80179b30
Function Address = 0x80127438
Function Address = 0x8012d734
Function Address = 0x80100a00
Function Address = 0xe0071004
Function Address = 0x8016ce0c
Function Address = 0x801223a0

Instruction dump:
41a2fe9c 812300ec 800200ec 7f890000 409efe8c 80010014 540b07b9 40a2fe80
4bfffe6c 80780290 7f64db78 4804ea35 <807f002c> 38800000 38a00080 3863000c
```

For detailed information about the command output, see Table 2.

Related commands

reset kernel starvation

display kernel starvation configuration

Use **display kernel starvation configuration** to display kernel thread starvation detection configuration.

Syntax

display kernel starvation configuration [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its ID. If you do not specify this option, the command displays kernel thread starvation detection configuration for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Examples

Display kernel thread starvation detection configuration.

```
<Sysname> display kernel starvation configuration
Thread starvation detection: Disabled
Starvation timer (in seconds): 10
Threads excluded from monitoring: 1
  TID:    123   Name: co0
```

Table 5 Command output

Field	Description
Starvation timer (in seconds): *n*	Time interval (in seconds) to identify a kernel thread starvation. A kernel thread starvation occurs if a kernel thread does not run within *n* seconds.
Threads excluded from monitoring	Kernel threads excluded from kernel thread starvation detection.
Name	Kernel thread name.
TID	Kernel thread number.

Related commands

monitor kernel starvation enable

monitor kernel starvation exclude-thread

monitor kernel starvation time

display process

Use **display process** to display process state information.

Syntax

display process [**all** | **job** *job-id* | **name** *process-name*] [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

all: Specifies all processes. With the **all** keyword or without any parameters, the command displays state information for all processes.

job *job-id*: Specifies a process by its job ID, in the range of 1 to 2147483647. Each process has a fixed job ID.

name *process-name*: Specifies a process by its name, a case-insensitive string of 1 to 15 characters that must not contain question marks or spaces.

slot *slot-number*: Specifies an IRF member device by its ID. If you do not specify this option, the command displays process state information for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Examples

Display state information for the process **scmd**.

```
<Sysname> display process name scmd
                            Job ID: 1
                               PID: 1
                        Parent JID: 0
                        Parent PID: 0
                    Executable path: /sbin/scmd
                           Instance: 0
                            Respawn: OFF
                      Respawn count: 1
             Max. spawns per minute: 0
                       Last started: Wed Jun  1 14:45:46 2013
                      Process state: sleeping
                          Max. core: 0
                               ARGS: -
   TID  LAST_CPU    Stack      PRI    State   HH:MM:SS:MSEC  Name
     1       0          0K      120       S     0:0:5:220      scmd
```

Table 6 Command output

Field	Description
Job ID	Job ID of the process. The job ID never changes.
PID	Number of the process. The number identifies the process, and it might change as the process restarts.
Parent JID	Job ID of the parent process.
Parent PID	Number of the parent process.
Executable path	Executable path of the process. For a kernel thread, this field displays a hyphen (-).
Instance	Instance number of the process. Whether a process can run multiple instances depends on the software implementation.
Respawn	Indicates whether the process restarts when an error occurs: • **ON**—The process automatically restarts. • **OFF**—The process does not automatically restarts.
Respawn count	Times that the process has restarted. The starting value is 1.
Max. spawns per minute	Maximum number of times that the process can restart within one minute. If the threshold is reached, the system automatically shuts down the process.
Last started	Time when the most recent restart occurred.
Process state	State of the process:

	• **running**—Running or waiting in the queue. • **sleeping**—Interruptible sleep. • **traced** or **stopped**—Stopped. • **uninterruptible sleep**—Uninterruptible sleep. • **zombie**—The process has quit, but some resources are not released.
Max. core	Maximum number of core dump files that the process can create. 0 indicates that the process never creates a core dump file. A process creates a core dump file after it abnormally restarts. If the number of core dump files reaches the maximum value, no more core dump files are created. Core dump files are helpful for troubleshooting.
ARGS	Parameters carried by the process during startup. If the process carries no parameters, this field displays a hyphen (-).
TID	Thread ID.
LAST_CPU	Number of the CPU on which the process is last scheduled.
Stack	Stack size.
PRI	Thread priority.
State	Thread state: • **R**—Running. • **S**—Sleeping. • **T**—Traced or stopped. • **D**—Uninterruptible sleep. • **Z**—Zombie.
HH:MM:SS:MSEC	Running time since the most recent start.
Name	Process name.

Display state information for all processes.

```
<Sysname> display process all
    JID    PID %CPU %MEM STAT PRI THIRD TTY HH:MM:SS COMMAND
      1      1  0.0  0.0   S  120   N   -  00:00:04 scmd
      2      2  0.0  0.0   S  115   N   -  00:00:00 [kthreadd]
      3      3  0.0  0.0   S   99   N   -  00:00:00 [migration/0]
      4      4  0.0  0.0   S  115   N   -  00:00:05 [ksoftirqd/0]
      5      5  0.0  0.0   S   99   N   -  00:00:00 [watchdog/0]
      6      6  0.0  0.0   S  115   N   -  00:00:00 [events/0]
      7      7  0.0  0.0   S  115   N   -  00:00:00 [khelper]
      8      8  0.0  0.0   S  115   N   -  00:00:00 [kblockd/0]
      9      9  0.0  0.0   S  115   N   -  00:00:00 [ata/0]
     10     10  0.0  0.0   S  115   N   -  00:00:00 [ata_aux]
     11     11  0.0  0.0   S  115   N   -  00:00:00 [kseriod]
     12     12  0.0  0.0   S  120   N   -  00:00:00 [vzmond]
     13     13  0.0  0.0   S  120   N   -  00:00:00 [pdflush]
     14     14  0.0  0.0   S  120   N   -  00:00:00 [pdflush]
     15     15  0.0  0.0   S  115   N   -  00:00:00 [kswapd0]
     16     16  0.0  0.0   S  115   N   -  00:00:00 [aio/0]
     17     17  0.0  0.0   S  115   N   -  00:00:00 [scsi_eh_0]
     18     18  0.0  0.0   S  115   N   -  00:00:00 [scsi_eh_1]
     19     19  0.0  0.0   S  115   N   -  00:00:00 [scsi_eh_2]
```

```
     35     35  0.0  0.0   D  100   N   -  00:00:00 [lipc_topology]
---- More ----
```

Table 7 Command output

Field	Description
JID	Job ID of a process. It never changes.
PID	Number of a process.
%CPU	CPU usage in percentage (%).
%MEM	Memory usage in percentage (%).
STAT	State of a process: • **R**—Running. • **S**—Sleeping. • **T**—Traced or stopped. • **D**—Uninterruptible sleep. • **Z**—Zombie.
PRI	Priority of a process for scheduling.
THIRD	This field is not supported in the current software version. Whether the process is a third party process: • **Y**—The process is a third party process. • **N**—The process is not a third party process.
TTY	TTY used by a process.
HH:MM:SS	Running time since the most recent start. If the running time reaches or exceeds 100 hours, this field displays only the number of hours.
COMMAND	Name and parameters of a process. If square brackets ([ ]) exist in a process name, the process is a kernel thread.

display process cpu

Use **display process cpu** to display CPU usage for all processes.

Syntax

display process cpu [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Examples

Display CPU usage for all processes.

```
<Sysname> display process cpu
```

```
CPU utilization in 5 secs: 16.8%; 1 min: 4.7%; 5 mins: 4.7%
    JID      5Sec      1Min      5Min    Name
      1      0.0%      0.0%      0.0%    scmd
      2      0.0%      0.0%      0.0%    [kthreadd]
      3      0.1%      0.0%      0.0%    [ksoftirqd/0]
```

...

Table 8 Command output

Field	Description
CPU utilization in 5 secs: 16.8%; 1 min: 4.7%; 5 mins: 4.7%	System CPU usage within the last 5 seconds, 1 minute, and 5 minutes.
JID	Job ID of a process. It never changes.
5Sec	CPU usage of the process within the last 5 seconds.
1Min	CPU usage of the process within the last minute.
5Min	CPU usage of the process within the last 5 minutes.
Name	Name of the process. If square brackets ([ ]) exist in a process name, the process is a kernel thread.

display process log

Use **display process log** to display log information for all user processes.

Syntax

display process log [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Examples

Display log information for all user processes.

```
<Sysname> display process log
Process       JobID  PID    Abort Core Exit Kill StartTime      EndTime
knotify       92     92     N     N    0    36   12-17 07:10:27 12-17 07:10:27
knotify       93     93     N     N    0    --   12-17 07:10:27 12-17 07:10:27
automount     94     94     N     N    0    --   12-17 07:10:27 12-17 07:10:28
knotify       111    111    N     N    0    --   12-17 07:10:28 12-17 07:10:28
comsh         121    121    N     N    0    --   12-17 07:10:30 12-17 07:10:30
knotify       152    152    N     N    0    --   12-17 07:10:31 12-17 07:10:31
autocfgd      155    155    N     N    0    --   12-17 07:10:31 12-17 07:10:31
```

```
pkg_update    122    122    N     N    0    --   12-17 07:10:30 12-17 07:10:31
```

Table 9 Command output

Field	Description
Process	Name of a user process.
JobID	Job ID of a user process.
PID	ID of a user process.
Abort	Indicates whether the process exited abnormally: • **Y**—Yes. • **N**—No.
Core	Indicates whether the process can generate core dump files: • **Y**—Yes. • **N**—No.
Exit	Process exit code. This field displays two hyphens (--) if the process was killed by a signal.
Kill	Code of the signal that killed the process. This field displays two hyphens (--) if the process exited instead of being killed.
StartTime	Time when the user process started.
EndTime	Time when the user process ended.

display process memory

Use **display process memory** to display memory usage for all user processes.

Syntax

display process memory [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

When a user process starts, it requests the following types of memory from the system:

- **Text memory**—Stores code for the user process.
- **Data memory**—Stores data for the user process.
- **Stack memory**—Stores temporary data.
- **Dynamic memory**—Heap memory dynamically assigned and released by the system according to the needs of the user process. To view dynamic memory information, execute the **display process memory heap** command.

Examples

Display memory usage for all user processes.

```
<Sysname> display process memory
   JID       Text      Data      Stack    Dynamic    Name
     1        384      1800         16         36    scmd
     2          0         0          0          0    [kthreadd]
     3          0         0          0          0    [ksoftirqd/0]
     4          0         0          0          0    [watchdog/0]
     5          0         0          0          0    [events/0]
     6          0         0          0          0    [khelper]
    29          0         0          0          0    [kblockd/0]
    49          0         0          0          0    [vzmond]
    52          0         0          0          0    [pdflush]
---- More ----
```

Table 10 Command output

Field	Description
JID	Job ID of a process. It never changes.
Text	Text memory used by the user process, in KB. The value for a kernel thread is 0.
Data	Data memory used by the user process, in KB. The value for a kernel thread is 0.
Stack	Stack memory used by the user process, in KB. The value for a kernel thread is 0.
Dynamic	Dynamic memory used by the user process, in KB. The value for a kernel thread is 0.
Name	Name of the user process. If square brackets ([ ]) exist in a process name, the process is a kernel thread.

Related commands

display process memory heap

display process memory heap address

display process memory heap size

display process memory heap

Use **display process memory heap** to display heap memory usage for a user process.

Syntax

display process memory heap job *job-id* [**verbose**] [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

job *job-id*: Specifies a user process by its job ID, in the range of 1 to 2147483647.

verbose: Displays detailed information. If you do not specify this keyword, the command displays brief information.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

Heap memory comprises fixed-sized blocks such as 16-byte or 64-byte blocks. It stores data and variables used by the user process. When a user process starts, the system dynamically allocates heap memory to the process.

Each memory block has an address represented in hexadecimal format, which can be used to access the memory block. You can view memory block addresses by using the **display process memory heap size** command, and view memory block contents by using the **display process memory heap address** command.

Examples

Display brief information about heap memory usage for the process identified by job ID 1.

```
<Sysname> display process memory heap job 1
Total virtual memory heap space(in bytes) :  2228224
Total physical memory heap space(in bytes) :  262144
Total allocated memory(in bytes)          :  161576
```

Display detailed information about heap memory usage for the process identified by job ID 1.

```
<Sysname> display process memory heap job 1 verbose
Heap usage:
Size       Free      Used      Total     Free Ratio
16         8         52        60        13%
64         3         1262      1265      0.2%
128        2         207       209       1%
512        3         55        58        5.1%
4096       3         297       300       1%
8192       1         19        20        5%
81920      0         1         1         0%
Summary:
Total virtual memory heap space (in bytes)  :  2293760
Total physical memory heap space (in bytes) :  58368
Total allocated memory (in bytes)           :  42368
```

Table 11 Command output

Field	Description
Size	Size of each memory block, in bytes.
Free	Number of free memory blocks.
Used	Number of used memory blocks.
Total	Total number of memory blocks.
Free Ratio	Ratio of free memory to total memory. It helps identify fragment information.

Related commands

display process memory

display process memory heap address

display process memory heap size

display process memory heap address

Use **display process memory heap address** to display heap memory content starting from a specified memory block for a process.

Syntax

display process memory heap job *job-id* **address** *starting-address* **length** *memory-length* [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

job *job-id*: Specifies a user process by its job ID, in the range of 1 to 2147483647.

address *starting-address*: Specifies the starting memory block by its address.

length *memory-length*: Specifies the memory block length in the range of 1 to 1024 bytes.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

When a user process runs abnormally, the command helps locate the problem.

Examples

Display 128-byte memory block content starting from the memory block 0xb7e30580 for the process **job 1**.

```
<Sysname> display process memory heap job 1 address b7e30580 length 128
B7E30580:  14 00 EF FF 00 00 00 00 E4 39 E2 B7 7C 05 E3 B7  .........9..|...
B7E30590:  14 00 EF FF 2F 73 62 69 6E 2F 73 6C 62 67 64 00  ..../sbin/slbgd.
B7E305A0:  14 00 EF FF 00 00 00 00 44 3B E2 B7 8C 05 E3 B7  ........D;......
B7E305B0:  14 00 EF FF 2F 73 62 69 6E 2F 6F 73 70 66 64 00  ..../sbin/ospfd.
B7E305C0:  14 00 EF FF 00 00 00 00 A4 3C E2 B7 AC 05 E3 B7  .........<......
B7E305D0:  14 00 EF FF 2F 73 62 69 6E 2F 6D 73 74 70 64 00  ..../sbin/mstpd.
B7E305E0:  14 00 EF FF 00 00 00 00 04 3E E2 B7 CC 05 E3 B7  .........>......
B7E305F0:  14 00 EF FF 2F 73 62 69 6E 2F 6E 74 70 64 00 00  ..../sbin/ntpd..
```

Related commands

display process memory heap

display process memory heap size

display process memory heap size

Use **display process memory heap size** to display the addresses of heap memory blocks with a specified size used by a process.

Syntax

display process memory heap job *job-id* **size** *memory-size* [**offset** *offset-size*] [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

job *job-id*: Specifies a process by its job ID, in the range of 1 to 2147483647.

size *memory-size*: Specifies the memory block size in the range of 1 to 4294967295.

offset *offset-size*: Specifies an offset in the range of 0 to 4294967295. The default value is 128. For example, suppose the system allocates 100 16-byte memory blocks to process job 1, and the process has used 66 blocks. Then if you execute the **display process memory heap job** *1* **size** *16* **offset** *50* command, the output shows the addresses of the 51st through 66th 16-byte blocks used by the process.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

The command displays memory block addresses in hexadecimal format. To view memory block content, execute the **display process memory heap address** command.

Examples

Display the addresses of 16-byte memory blocks used by process job 1.

```
<Sysname> display process memory heap job 1 size 16
0xb7e300c0  0xb7e300d0  0xb7e300e0  0xb7e300f0
0xb7e30100  0xb7e30110  0xb7e30120  0xb7e30130
0xb7e30140  0xb7e30150  0xb7e30160  0xb7e30170
0xb7e30180  0xb7e30190  0xb7e301a0  0xb7e301b0
0xb7e301c0  0xb7e301d0  0xb7e301e0  0xb7e301f0
0xb7e30200  0xb7e30210  0xb7e30220  0xb7e30230
```

Display the addresses of 16-byte memory blocks starting from the fifth block used by process job 1.

```
<Sysname> display process memory heap job 1 size 16 offset 4
0xb7e30100  0xb7e30110  0xb7e30120  0xb7e30130
0xb7e30140  0xb7e30150  0xb7e30160  0xb7e30170
0xb7e30180  0xb7e30190  0xb7e301a0  0xb7e301b0
0xb7e301c0  0xb7e301d0  0xb7e301e0  0xb7e301f0
0xb7e30200  0xb7e30210  0xb7e30220  0xb7e30230
```

Related commands

display process memory heap

display process memory heap address

exception filepath

Use **exception filepath** to specify the directory for saving core dump files.

Use **undo exception filepath** to remove the specified directory.

Syntax

exception filepath *directory*

undo exception filepath *directory*

Default

The directory for saving core dump files is the root directory of the default file system. For more information about the default file system, see file system management in *Fundamentals Configuration Guide*.

Views

User view

Predefined user roles

network-admin

Parameters

directory: Specifies the directory for saving core dump files. The directory must be the root directory of a file system.

Usage guidelines

The system will save core dump files to the **core** folder in the specified directory on the master. If the **core** folder does not exist in the specified directory, the system creates the **core** folder before saving core dump files.

You can use the command to change the directory if there are different types of storage media on the device.

If no directory is specified or the specified directory is not accessible, the system cannot save core dump files.

Examples

Set the directory for saving core dump files to flash:/.

```
<Sysname> exception filepath flash:/
```

Related commands

display exception filepath

process core

monitor kernel deadloop action

Use **monitor kernel deadloop action** to specify the action to be taken in response to a kernel thread deadloop.

Use **undo monitor kernel deadloop action** to restore the default.

Syntax

monitor kernel deadloop action { **reboot** | **record-only** } [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor kernel deadloop action [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

The kernel thread deadloop protection action is **reboot**.

Views

System view

Predefined user roles

network-admin

Parameters

reboot: Logs the event and reboots the specified slot or CPU.

record-only: Logs the event.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command specifies the action for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

Use this command only under the guidance of H3C technical support staff. Inappropriate configuration can cause system breakdown. As a best practice, leave the default unchanged.

Examples

Set the kernel thread deadloop protection action to **reboot** for slot 1.

```
<Sysname> system-view
[Sysname] monitor kernel deadloop action reboot slot 1
```

Related commands

display kernel deadloop configuration

monitor kernel deadloop enable

monitor kernel deadloop enable

Use **monitor kernel deadloop enable** to enable kernel thread deadloop detection.

Use **undo monitor kernel deadloop enable** to disable kernel thread deadloop detection.

Syntax

monitor kernel deadloop enable [**slot** *slot-number* [**cpu** *cpu-number* [**core** *core-number*&<1-64>]]]

undo monitor kernel deadloop enable [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

Kernel thread deadloop detection is enabled.

Views

System view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its ID. If you do not specify this option, the master device is specified.

cpu *cpu-number*: Specifies a CPU by its number.

core *core-number*&<1-64>]: Specifies a maximum of 64 CPU cores. If you do not specify this option, the command applies to all cores of the specified CPU.

Usage guidelines

CAUTION:

Use this command only under the guidance of H3C technical support staff. Inappropriate configuration can cause system breakdown. As a best practice, leave the default unchanged.

Kernel threads share resources in kernel space. If a kernel thread monopolizes the CPU for a long time, other threads cannot run, resulting in a deadloop.

This command enables the device to detect deadloops. If a thread occupies the CPU regularly, the device considers that a deadloop has occurred.

Examples

Enable kernel thread deadloop detection.

```
<Sysname> system-view
[Sysname] monitor kernel deadloop enable
```

Related commands

display kernel deadloop

display kernel deadloop configuration

monitor kernel deadloop action

monitor kernel deadloop exclude-thread

monitor kernel deadloop time

monitor kernel deadloop exclude-thread

Use **monitor kernel deadloop exclude-thread** to disable kernel thread deadloop detection for a kernel thread.

Use **undo monitor kernel deadloop exclude-thread** to enable kernel thread deadloop detection for a kernel thread.

Syntax

monitor kernel deadloop exclude-thread *tid* [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor kernel deadloop exclude-thread [*tid*] [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

Kernel thread deadloop detection monitors all kernel threads.

Views

System view

Predefined user roles

network-admin

Parameters

tid: Specifies a kernel thread by its ID, in the range of 1 to 2147483647. If no kernel thread is specified for the undo command, the default is restored.

slot *slot-number*: Specifies an IRF member device by its ID. If you do not specify this option, the master device is specified.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

Use this command only under the guidance of H3C technical support staff. Inappropriate configuration can cause system breakdown. As a best practice, leave the default unchanged.

You can disable kernel thread deadloop detection for up to 128 kernel threads by executing the command.

Examples

Disable kernel thread deadloop detection for kernel thread 15.

```
<Sysname> system-view
[Sysname]monitor kernel deadloop exclude-thread 15
```

Related commands

display kernel deadloop configuration

display kernel deadloop

monitor kernel deadloop enable

monitor kernel deadloop time

Use **monitor kernel deadloop time** to set the interval for identifying a kernel thread deadloop.

Use **undo monitor kernel deadloop time** to restore the default.

Syntax

monitor kernel deadloop time *time* [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor kernel deadloop time [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

The interval for identifying a kernel thread deadloop is 20 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

time *time*: Specifies the interval for identifying a kernel thread deadloop, in the range of 1 to 65535 seconds.

slot *slot-number*: Specifies an IRF member device by its ID. If you do not specify this option, the master device is specified.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

Use this command only under the guidance of H3C technical support staff. Inappropriate configuration can cause system breakdown. As a best practice, leave the default unchanged.

If a kernel thread runs for the specified interval, kernel thread deadloop detection considers that a deadloop has occurred.

Examples

Set the interval for identifying a kernel thread deadloop to 8 seconds.

```
<Sysname> system-view
[Sysname] monitor kernel deadloop time 8
```

Related commands

display kernel deadloop configuration

display kernel deadloop

monitor kernel deadloop enable

monitor kernel starvation enable

Use **monitor kernel starvation enable** to enable kernel thread starvation detection.

Use **undo monitor kernel starvation enable** to disable kernel thread starvation detection.

Syntax

monitor kernel starvation enable [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor kernel starvation enable [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

Kernel thread starvation detection is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its ID. If you do not specify this option, the master device is specified.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

CAUTION:

Use this command only under the guidance of H3C technical support staff. Inappropriate configuration can cause system breakdown. As a best practice, leave the default unchanged.

Starvation occurs when a thread is unable to access shared resources.

The command enables the system to detect and report thread starvation. If a thread is not executed within an interval, the system considers that a starvation has occurred, and outputs a starvation message.

Thread starvation does not impact system operation. A starved thread can automatically run when certain conditions are met.

Examples

Enable kernel thread starvation detection.

```
<Sysname> system-view
[Sysname] monitor kernel starvation enable
```

Related commands

display kernel starvation configuration

display kernel starvation

monitor kernel starvation time

monitor kernel starvation exclude-thread

monitor kernel starvation exclude-thread

Use **monitor kernel starvation exclude-thread** to disable kernel thread starvation detection for a kernel thread.

Use **undo monitor kernel starvation exclude-thread** to enable kernel thread starvation detection for a kernel thread.

Syntax

monitor kernel starvation exclude-thread *tid* [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor kernel starvation exclude-thread [*tid*] [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

Kernel thread starvation detection, if enabled, monitors all kernel threads.

Views

System view

Predefined user roles

network-admin

Parameters

tid: Specifies a kernel thread by its ID, in the range of 1 to 2147483647. If no kernel thread is specified for the undo command, the default is restored.

slot *slot-number*: Specifies an IRF member device by its ID. If you do not specify this option, the master device is specified.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

Use this command only under the guidance of H3C technical support staff. Inappropriate configuration can cause system breakdown. As a best practice, leave the default unchanged.

You can disable kernel thread starvation detection for up to 128 kernel threads by executing the command.

Examples

Disable kernel thread starvation detection for kernel thread 15.

```
<Sysname> system-view
[Sysname] monitor kernel starvation exclude-thread 15
```

Related commands

display kernel starvation

display kernel starvation configuration

monitor kernel starvation enable

monitor kernel starvation time

Use **monitor kernel starvation time** to set the interval for identifying a kernel thread starvation.

Use **undo monitor kernel starvation time** to restore the default.

Syntax

monitor kernel starvation time *time* [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor kernel starvation time [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

The interval for identifying a kernel thread starvation is 120 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

time *time*: Specifies the interval for identifying a kernel thread starvation, in the range of 1 to 65535 seconds.

slot *slot-number*: Specifies an IRF member device by its ID. If you do not specify this option, the master device is specified.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

Use this command only under the guidance of H3C technical support staff. Inappropriate configuration can cause system breakdown. As a best practice, leave the default unchanged.

If a thread is not executed within the specified interval, the system considers that a starvation has occurred, and outputs a starvation message.

Examples

Set the interval for identifying a kernel thread starvation to 120 seconds.

```
<Sysname> system-view
[Sysname] monitor kernel starvation time 120
```

Related commands

display kernel starvation

display kernel starvation configuration

monitor kernel starvation enable

monitor process

Use **monitor process** to display process statistics.

Syntax

monitor process [**dumbtty**] [**iteration** *number*] [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

Parameters

dumbtty: Specifies dumbtty mode. In this mode, the command displays process statistics in descending order of CPU usage without refreshing statistics. If you do not specify this keyword, the command displays statistics for the top 10 processes in descending order of CPU usage in an interactive mode, and refreshes statistics every 5 seconds by default.

iteration *number*: Specifies the number of display times, in the range of 1 to 4294967295. If you specify the **dumbtty** keyword, the *number* argument is 1 by default. If neither the **dumbtty** keyword nor the *number* argument is specified, there is no limit to the display times and process statistics are refreshed every 5 seconds.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

If you do not specify the **dumbtty** keyword, the command displays process statistics in an interactive mode. In this mode, the system automatically determines the number of displayed processes according to the screen size, and does not display exceeding processes. You can also input interactive commands as shown in Table 12 to perform relevant operations.

Table 12 Interactive commands

Commands	Description
? or h	Displays help information that includes available interactive commands.
1	Displays state information for physical CPUs. For example, if you enter 1 for the first time, the state of each physical CPU is displayed in a separate row. If you enter 1 again, the average value of all CPU states is displayed. If you enter 1 for the third time, separate states are displayed. By default, the average value of all CPU states is displayed.
c	Sorts processes by CPU usage in descending order, which is the default setting.
d	Sets the interval for refreshing process statistics, in the range of 1 to 2147483647 seconds. The default value is 5 seconds.
f	Sorts processes by the number of open files in descending order. Files are identified by file descriptors (FDs).
k	Kills a process. Because the command can impact system operation, be cautious to use it.
l	Refreshes the screen.
m	Sorts processes by memory usage in descending order.
n	Changes the maximum number of processes displayed within a screen, in the range of 0 to 2147483647. The default value is 10. A value of 0 means no limit. Only processes not exceeding the screen size can be displayed.
q	Quits the interactive mode.

Commands	Description
t	Sorts processes by running time in descending order.
<	Moves sort field to the next left column.
>	Moves sort field to the next right column.

Examples

Display process statistics in dumbtty mode. In this mode, the system displays process statistics once, and then returns to command view.

```
<Sysname> monitor process dumbtty
 76 processes; 103 threads; 687 fds
Thread states: 1 running, 102 sleeping, 0 stopped, 0 zombie
CPU states: 77.16% idle, 0.00% user, 14.96% kernel, 7.87% interrupt
Memory: 496M total, 341M available, page size 4K
    JID    PID  PRI  State  FDs    MEM  HH:MM:SS    CPU   Name
   1047   1047  120    R     9   1420K  00:02:23  13.53%  diagd
      1      1  120    S    17   1092K  00:00:20   7.61%  scmd
   1000   1000  115    S     0      0K  00:00:09   0.84%  [sock/1]
   1026   1026  120    S    20  26044K  00:00:05   0.84%  syslogd
      2      2  115    S     0      0K  00:00:00   0.00%  [kthreadd]
      3      3   99    S     0      0K  00:00:00   0.00%  [migration/0]
      4      4  115    S     0      0K  00:00:06   0.00%  [ksoftirqd/0]
      5      5   99    S     0      0K  00:00:00   0.00%  [watchdog/0]
      6      6  115    S     0      0K  00:00:01   0.00%  [events/0]
      7      7  115    S     0      0K  00:00:00   0.00%  [khelper]
   4797   4797  120    S     8  28832K  00:00:02   0.00%  comsh
   5117   5117  120    S     8   1496K  00:00:00   0.00%  top

<Sysname>
```

Display process statistics twice in dumbtty mode.

```
<Sysname> monitor process dumbtty iteration 2
76 processes; 103 threads; 687 fds
Thread states: 1 running, 102 sleeping, 0 stopped, 0 zombie
CPU states: 44.84% idle, 0.51% user, 39.17% kernel, 15.46% interrupt
Memory: 496M total, 341M available, page size 4K
    JID    PID  PRI  State  FDs    MEM  HH:MM:SS    CPU   Name
   1047   1047  120    R     9   1420K  00:02:30  37.11%  diagd
      1      1  120    S    17   1092K  00:00:21  11.34%  scmd
   1000   1000  115    S     0      0K  00:00:09   2.06%  [sock/1]
   1026   1026  120    S    20  26044K  00:00:05   1.54%  syslogd
   1027   1027  120    S    12   9280K  00:01:12   1.03%  devd
      4      4  115    S     0      0K  00:00:06   0.51%  [ksoftirqd/0]
   1009   1009  115    S     0      0K  00:00:08   0.51%  [karp/1]
   1010   1010  115    S     0      0K  00:00:13   0.51%  [kND/1]
   5373   5373  120    S     8   1496K  00:00:00   0.51%  top
      2      2  115    S     0      0K  00:00:00   0.00%  [kthreadd]
      3      3   99    S     0      0K  00:00:00   0.00%  [migration/0]
      5      5   99    S     0      0K  00:00:00   0.00%  [watchdog/0]
```

```
     6      6  115    S     0      0K  00:00:01   0.00%  [events/0]
     7      7  115    S     0      0K  00:00:00   0.00%  [khelper]
  4796   4796  120    S    11   2744K  00:00:00   0.00%  login
  4797   4797  120    S     8  28832K  00:00:03   0.00%  comsh
```

Five seconds later, the system refreshes process statistics as follows (which is the same as executing the **`monitor process dumbtty`** command twice at a 5-second interval):

```
76 processes; 103 threads; 687 fds
Thread states: 1 running, 102 sleeping, 0 stopped, 0 zombie
CPU states: 78.71% idle, 0.16% user, 14.86% kernel, 6.25% interrupt
Memory: 496M total, 341M available, page size 4K
    JID    PID  PRI  State  FDs    MEM  HH:MM:SS    CPU   Name
   1047   1047  120    R     9   1420K  00:02:31  14.25%  diagd
      1      1  120    S    17   1092K  00:00:21   4.25%  scmd
   1027   1027  120    S    12   9280K  00:01:12   1.29%  devd
   1000   1000  115    S     0      0K  00:00:09   0.37%  [sock/1]
   5373   5373  120    S     8   1500K  00:00:00   0.37%  top
      6      6  115    S     0      0K  00:00:01   0.18%  [events/0]
   1009   1009  115    S     0      0K  00:00:08   0.18%  [karp/1]
   1010   1010  115    S     0      0K  00:00:13   0.18%  [kND/1]
   4795   4795  120    S    11   2372K  00:00:01   0.18%  telnetd
      2      2  115    S     0      0K  00:00:00   0.00%  [kthreadd]
      3      3   99    S     0      0K  00:00:00   0.00%  [migration/0]
      4      4  115    S     0      0K  00:00:06   0.00%  [ksoftirqd/0]
      5      5   99    S     0      0K  00:00:00   0.00%  [watchdog/0]
      7      7  115    S     0      0K  00:00:00   0.00%  [khelper]
   4796   4796  120    S    11   2744K  00:00:00   0.00%  login
   4797   4797  120    S     8  28832K  00:00:03   0.00%  comsh


<Sysname>
```

Display process statistics in interactive mode.

```
<Sysname> monitor process
76 processes; 103 threads; 687 fds
Thread states: 1 running, 102 sleeping, 0 stopped, 0 zombie
CPU states: 78.98% idle, 0.16% user, 14.57% kernel, 6.27% interrupt
Memory: 496M total, 341M available, page size 4K
    JID    PID  PRI  State  FDs    MEM  HH:MM:SS    CPU   Name
   1047   1047  120    R     9   1420K  00:02:39  14.13%  diagd
      1      1  120    S    17   1092K  00:00:23   3.98%  scmd
   1027   1027  120    S    12   9280K  00:01:13   1.44%  devd
   1000   1000  115    S     0      0K  00:00:09   0.36%  [sock/1]
   1009   1009  115    S     0      0K  00:00:09   0.36%  [karp/1]
      4      4  115    S     0      0K  00:00:06   0.18%  [ksoftirqd/0]
   1010   1010  115    S     0      0K  00:00:13   0.18%  [kND/1]
   4795   4795  120    S    11   2372K  00:00:01   0.18%  telnetd
   5491   5491  120    S     8   1500K  00:00:00   0.18%  top
      2      2  115    S     0      0K  00:00:00   0.00%  [kthreadd]
```

The system refreshes process statistics every 5 seconds. You can enter interactive commands to perform operation as follows:

- Enter **h** or a question mark (?) to display help information as follows:

```
Help for interactive commands:
      ?,h    Show the available interactive commands
        1    Toggle SMP view: '1' single/separate states
        c    Sort by the CPU field(default)
        d    Set the delay interval between screen updates
        f    Sort by number of open files
        k    Kill a job
        l    Refresh the screen
        m    Sort by memory used
        n    Set the maximum number of processes to display
        q    Quit the interactive display
        t    Sort by run time of processes since last restart
        <    Move sort field to the next left column
        >    Move sort field to the next right column
Press any key to continue
```

- Enter **d**, and then enter a number to modify the refresh interval. If you enter **3**, statistics are refreshed every 3 seconds.

```
Enter the delay interval between updates(1~2147483647): 3
```

- Enter **n**, and then enter a number to modify the maximum number of displayed processes. If you enter **5**, statistics for five processes are displayed.

```
Enter the max number of processes to display(0 means unlimited): 5
87 processes; 113 threads; 735 fds
Thread states: 2 running, 111 sleeping, 0 stopped, 0 zombie
CPU states: 86.57% idle, 0.83% user, 11.74% kernel, 0.83% interrupt
Memory: 755M total, 414M available, page size 4K
    JID    PID  PRI  State  FDs    MEM  HH:MM:SS    CPU   Name
    864    864  120    S    24  27020K  00:00:43   8.95%  syslogd
   1173   1173  120    R    24   2664K  00:00:01   2.37%  top
    866    866  120    S    18  10276K  00:00:09   0.69%  devd
      1      1  120    S    16   1968K  00:00:04   0.41%  scmd
    881    881  120    S     8   2420K  00:00:07   0.41%  diagd
```

- Enter **f** to sort processes by FDs in descending order. (You can also enter command **c**, **m**, or **t** to sort processes.)

```
87 processes; 113 threads; 735 fds
Thread states: 1 running, 112 sleeping, 0 stopped, 0 zombie
CPU states: 90.66% idle, 0.88% user, 5.77% kernel, 2.66% interrupt
Memory: 755M total, 414M available, page size 4K
    JID    PID  PRI  State  FDs    MEM  HH:MM:SS    CPU   Name
    862    862  120    S    61   5384K  00:00:01   0.00%  dbmd
    905    905  120    S    35   2464K  00:00:02   0.00%  ipbased
    863    863  120    S    31   1956K  00:00:00   0.00%  had
    884    884  120    S    31  30600K  00:00:00   0.00%  lsmd
    889    889  120    S    29  61592K  00:00:00   0.00%  routed
```

- Enter **k** and then enter a JID to kill a process. If you enter **884**, the process with the JID of 884 is killed.

```
Enter the JID to kill: 884
84 processes; 107 threads; 683 fds
Thread states: 1 running, 106 sleeping, 0 stopped, 0 zombie
```

```
CPU states: 59.03% idle, 1.92% user, 37.88% kernel, 1.15% interrupt
Memory: 755M total, 419M available, page size 4K
    JID    PID  PRI  State  FDs    MEM  HH:MM:SS    CPU   Name
    862    862  120    S     56   5384K  00:00:01   0.00%  dbmd
    905    905  120    S     35   2464K  00:00:02   0.00%  ipbased
    863    863  120    S     30   1956K  00:00:00   0.00%  had
    889    889  120    S     29  61592K  00:00:00   0.00%  routed
   1160   1160  120    S     28  23096K  00:00:01   0.19%  sshd
```

- Enter **q** to quit interactive mode.

Table 13 Command output

Field	Description
84 processes; 107 threads; 683 fds	Numbers of processes, threads, and open files.
JID	Job ID of a process, which never changes.
PID	ID of a process.
PRI	Priority level of a process.
State	State of a process: • **R**—Running. • **S**—Sleeping. • **T**—Traced or stopped. • **D**—Uninterruptible sleep. • **Z**—Zombie.
FDs	Number of open files for a process.
MEM	Memory usage. It displays **0** for a kernel thread.
HH:MM:SS	Running time of a process since last restart.
CPU	CPU usage of a process.
Name	Name of a process. If square brackets ([ ]) exist in a process name, the process is a kernel thread.

monitor thread

Use **monitor thread** to display thread statistics.

Syntax

monitor thread [**dumbtty**] [**iteration** *number*] [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

Parameters

dumbtty: Specifies dumbtty mode. In this mode, the command displays all thread statistics in descending order of CPU usage without refreshing statistics. If you do not specify the keyword, the

command displays statistics for top 10 processes in descending order of CPU usage in an interactive mode, and refreshes statistics every 5 seconds by default.

iteration *number*: Specifies the number of display times, in the range of 1 to 4294967295. If you specify the **dumbtty** keyword, the *number* argument is 1 by default. If neither the **dumbtty** keyword nor the *number* argument is specified, there is no limit to the display times.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

If you do not specify the **dumbtty** keyword, the command displays thread statistics in an interactive mode. In this mode, the system automatically determines the number of displayed thread processes according to the screen size and does not display exceeding processes. You can also input interactive keywords as shown in Table 14 to perform relevant operations.

Table 14 Interactive keywords

Keyword	Description
? or h	Displays help information that includes available interactive keywords.
1	Displays one of the following items in turn when you press **1** again and again: • Values of parameters of physical CPUs. • Average values of parameters of all CPUs. By default, the command displays the average values of parameters of all CPUs.
c	Sorts statistics by CPU usage in descending order. By default, the command sorts statistics by CPU usage in descending order.
d	Sets the interval for refreshing statistics. The default interval is 5 seconds.
k	Kills a process. Because the command can impact system operation, be cautious when you use it.
l	Refreshes the screen.
n	Changes the maximum number of threads displayed within a screen, in the range of 0 to 2147483647. The default value is 10. A value of 0 means no limit. Only threads not exceeding the screen size can be displayed.
q	Quits interactive mode.
t	Sorts statistics by the running time since the latest startup.
<	Moves sort field to the next left column.
>	Moves sort field to the next right column.

Examples

Display thread statistics in dumbtty mode.

```
<Sysname> monitor thread dumbtty
84 processes; 107 threads
Thread states: 1 running, 106 sleeping, 0 stopped, 0 zombie
CPU states: 83.19% idle, 1.68% user, 10.08% kernel, 5.04% interrupt
Memory: 755M total, 417M available, page size 4K
    JID    TID  LAST_CPU  PRI  State  HH:MM:SS   MAX    CPU    Name
   1175   1175      0     120    R    00:00:00     1  10.75%   top
      1      1      0     120    S    00:00:06     1   2.68%   scmd
    881    881      0     120    S    00:00:09     1   2.01%   diagd
```

```
   776    776      0     120    S    00:00:01     0   0.67%   [DEVD]
   866    866      0     120    S    00:00:11     1   0.67%   devd
     2      2      0     115    S    00:00:00     0   0.00%   [kthreadd]
     3      3      0     115    S    00:00:01     0   0.00%   [ksoftirqd/0]
     4      4      0      99    S    00:00:00     1   0.00%   [watchdog/0]
     5      5      0     115    S    00:00:00     0   0.00%   [events/0]
     6      6      0     115    S    00:00:00     0   0.00%   [khelper]
   796    796      0     115    S    00:00:00     0   0.00%   [kip6fs/1]

<Sysname>
```

Display thread statistics in interactive mode.

```
<Sysname> monitor thread
84 processes; 107 threads
Thread states: 1 running, 106 sleeping, 0 stopped, 0 zombie
CPU states: 94.43% idle, 0.76% user, 3.64% kernel, 1.15% interrupt
Memory: 755M total, 417M available, page size 4K
    JID    TID  LAST_CPU  PRI  State  HH:MM:SS   MAX    CPU    Name
   1176   1176      0     120    R    00:00:01     1   3.42%   top
    866    866      0     120    S    00:00:12     1   0.85%   devd
    881    881      0     120    S    00:00:09     1   0.64%   diagd
      1      1      0     120    S    00:00:06     1   0.42%   scmd
   1160   1160      0     120    S    00:00:01     1   0.21%   sshd
      2      2      0     115    S    00:00:00     0   0.00%   [kthreadd]
      3      3      0     115    S    00:00:01     0   0.00%   [ksoftirqd/0]
      4      4      0      99    S    00:00:00     1   0.00%   [watchdog/0]
      5      5      0     115    S    00:00:00     0   0.00%   [events/0]
      6      6      0     115    S    00:00:00     0   0.00%   [khelper]
```

- Enter **h** or a question mark (?) to display help information as follows:

```
Help for interactive commands:
        ?,h      Show the available interactive commands
          1      Toggle SMP view: '1' single/separate states
          c      Sort by the CPU field(default)
          d      Set the delay interval between screen updates
          k      Kill a job
          l      Refresh the screen
          n      Set the maximum number of threads to display
          q      Quit the interactive display
          t      Sort by run time of threads since last restart
          <      Move sort field to the next left column
          >      Move sort field to the next right column
Press any key to continue
```

- Enter **d**, and then enter a number to modify the refresh interval. If you enter **3**, statistics are refreshed every 3 seconds.

```
Enter the delay interval between screen updates (1~2147483647): 3
```

- Enter **n**, and then enter a number to modify the maximum number of displayed threads. If you enter **5**, statistics for five threads are displayed.

```
Enter the max number of threads to display(0 means unlimited): 5
84 processes; 107 threads
```

```
Thread states: 1 running, 106 sleeping, 0 stopped, 0 zombie
CPU states: 93.26% idle, 0.99% user, 4.23% kernel, 1.49% interrupt
Memory: 755M total, 417M available, page size 4K
    JID    TID  LAST_CPU  PRI  State  HH:MM:SS   MAX    CPU    Name
   1176   1176      0     120    R    00:00:02     1   3.71%   top
      1      1      0     120    S    00:00:06     1   0.92%   scmd
    866    866      0     120    S    00:00:13     1   0.69%   devd
    881    881      0     120    S    00:00:10     1   0.69%   diagd
    720    720      0     115    D    00:00:01     0   0.23%   [TMTH]
```

- Enter **k** and then enter a JID to kill a thread. If you enter **881**, the thread with the JID of 881 is killed.

```
Enter the JID to kill: 881
83 processes; 106 threads
Thread states: 1 running, 105 sleeping, 0 stopped, 0 zombie
CPU states: 96.26% idle, 0.54% user, 2.63% kernel, 0.54% interrupt
Memory: 755M total, 418M available, page size 4K
    JID    TID  LAST_CPU  PRI  State  HH:MM:SS   MAX    CPU    Name
   1176   1176      0     120    R    00:00:04     1   1.86%   top
    866    866      0     120    S    00:00:14     1   0.87%   devd
      1      1      0     120    S    00:00:07     1   0.49%   scmd
    730    730      0       0    S    00:00:04     1   0.12%   [DIBC]
    762    762      0     120    S    00:00:22     1   0.12%   [MNET]
```

- Enter **q** to quit interactive mode.

Table 15 Command output

Field	Description
84 processes; 107 threads	Numbers of processes and threads.
JID	Job ID of a thread, which never changes.
TID	ID of a thread.
LAST_CPU	Number of the CPU on which the most recent thread scheduling occurs.
PRI	Priority level of a thread.
State	State of a thread: • **R**—Running. • **S**—Sleeping. • **T**—Traced or stopped. • **D**—Uninterruptible sleep. • **Z**—Zombie.
HH:MM:SS	Running time of a thread since last restart.
MAX	Longest time that a single thread scheduling occupies the CPU, in milliseconds.
CPU	CPU usage of a thread.
Name	Name of a thread. If square brackets ([ ]) exist in a thread name, the thread is a kernel thread.

process core

Use **process core** to enable or disable a process to generate core dump files for exceptions and set the maximum number of core dump files.

Syntax

process core { **maxcore** *value* | **off** } { **job** *job-id* | **name** *process-name* } [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

User view

Default

A process generates a core dump file for the first exception and does not generate any core dump files for subsequent exceptions.

Predefined user roles

network-admin

Parameters

off: Disables core dump file generation.

maxcore *value*: Enables core dump file generation and sets the maximum number of core dump files, in the range of 1 to 10.

name *process-name*: Specifies a process by its name, a case-insensitive string of 1 to 15 characters.

job *job-id*: Specifies a process by its job ID, in the range of 1 to 2147483647. The job ID does not change after the process restarts.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

The command applies to all instances of a process.

The command enables the system to generate a core dump file each time the specified process crashes until the maximum number of core dump files is reached. A core dump file records the exception information.

Because the core dump files consume system storage resources, you can disable core dump file generation for processes for which you do not need to review exception information.

Examples

Disable core dump file generation for process **routed**.

```
<Sysname> process core off name routed
```

Enable core dump file generation for process **routed** and set the maximum number of core dump files to 5.

```
<Sysname> process core maxcore 5 name routed
```

Related commands

display exception context

exception filepath

reset exception context

Use **reset exception context** to clear context information for process exceptions.

Syntax

reset exception context [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its ID. If you do not specify this option, the command clears context information for process exceptions on the IRF master device.

cpu *cpu-number*: Specifies a CPU by its number.

Examples

Clear context information for exceptions.

```
<Sysname> reset exception context
```

Related commands

display exception context

reset kernel deadloop

Use **reset kernel deadloop** to clear kernel thread deadloop information.

Syntax

reset kernel deadloop [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its ID. If you do not specify this option, the command clears kernel thread deadloop information for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Examples

Clear kernel thread deadloop information.

```
<Sysname> reset kernel deadloop
```

Related commands

display kernel deadloop

reset kernel exception

Use **reset kernel exception** to clear kernel thread exception information.

Syntax

reset kernel exception [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its ID. If you do not specify this option, the command clears kernel thread exception information for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Examples

Clear kernel thread exception information.

```
<Sysname> reset kernel exception
```

Related commands

display kernel exception

reset kernel reboot

Use **reset kernel reboot** to clear kernel thread reboot information.

Syntax

reset kernel reboot [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its ID. If you do not specify this option, the command clears kernel thread reboot information for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Examples

Clear kernel thread reboot information.

```
<Sysname> reset kernel reboot
```

Related commands

display kernel reboot

reset kernel starvation

Use **reset kernel starvation** to clear kernel thread starvation information.

Syntax

reset kernel starvation [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its ID. If you do not specify this option, the command clears kernel thread starvation information for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Examples

Clear kernel thread starvation information.

```
<Sysname> reset kernel starvation
```

Related commands

display kernel starvation

Contents

Port mirroring commands

display mirroring-group

Use **display mirroring-group** to display mirroring group information.

Syntax

display mirroring-group { *group-id* | **all** | **local** | **remote-destination** | **remote-source** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group-id: Specifies a mirroring group by its ID. The value range for this argument is 1 to 4.

all: Specifies all mirroring groups.

local: Specifies local mirroring groups.

remote-destination: Specifies remote destination groups.

remote-source: Specifies remote source groups.

Usage guidelines

Mirroring group information includes the type, status, and content of a mirroring group. It is sorted by mirroring group number.

Examples

Display information about all mirroring groups.

```
<Sysname> display mirroring-group all
Mirroring group 1:
    Type: Local
    Status: Active
    Mirroring port:
        GigabitEthernet1/0/1  Inbound
    Monitor port: GigabitEthernet1/0/2
```

Table 1 Command output

Field	Description
Mirroring group	Number of the mirroring group.
Type	Type of the mirroring group: • Local. • Remote source. • Remote destination.

Field	Description
Status	Status of the mirroring group: • **Active**—The mirroring group has taken effect. • **Incomplete**—The mirroring group configuration is not complete and does not take effect.
Mirroring port	Source port.
Monitor port	Destination port.

mirroring-group

Use **mirroring-group** to create a mirroring group.

Use **undo mirroring-group** to delete mirroring groups.

Syntax

mirroring-group *group-id* { **local** | **remote-destination** | **remote-source** }

undo mirroring-group { *group-id* | **all** | **local** | **remote-destination** | **remote-source** }

Default

No mirroring groups exist.

Views

System view

Predefined user roles

network-admin

Parameters

group-id: Specifies a mirroring group ID. The value range for this argument is 1 to 4.

local: Specifies local mirroring groups.

remote-destination: Specifies remote destination groups.

remote-source: Specifies remote source groups.

all: Specifies all mirroring groups.

Examples

Create local mirroring group 1.

```
<Sysname> system-view
[Sysname] mirroring-group 1 local
```

mirroring-group mirroring-port (interface view)

Use **mirroring-group mirroring-port** to configure a port as a source port for a mirroring group.

Use **undo mirroring-group mirroring-port** to restore the default.

Syntax

mirroring-group *group-id* **mirroring-port** { **both** | **inbound** | **outbound** }

undo mirroring-group *group-id* **mirroring-port**

Default

A port does not act as a source port for any mirroring groups.

Views

Interface view

Predefined user roles

network-admin

Parameters

group-id: Specifies a mirroring group by its ID. The value range for this argument is 1 to 4.

both: Mirrors both received and sent packets.

inbound: Mirrors only received packets.

outbound: Mirrors only sent packets.

Usage guidelines

You can configure source ports only for local mirroring groups and remote source groups.

A Layer 2 aggregate interface cannot be configured as a source port for a mirroring group.

Do not assign a source port of a mirroring group to the remote probe VLAN of the mirroring group.

The device supports only one mirroring group for outbound or bidirectional traffic mirroring

A port can act as a source port for only one mirroring group.

A source port cannot be used as a reflector port, monitor port, or egress port.

Examples

Create local mirroring group 1 to monitor the bidirectional traffic of the port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] mirroring-group 1 local
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mirroring-group 1 mirroring-port both
```

Create remote source group 2 to monitor the bidirectional traffic of the port GigabitEthernet 1/0/2.

```
<Sysname> system-view
[Sysname] mirroring-group 2 remote-source
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] mirroring-group 2 mirroring-port both
```

Related commands

mirroring-group

mirroring-group mirroring-port (system view)

Use **mirroring-group mirroring-port** to configure source ports for a mirroring group.

Use **undo mirroring-group mirroring-port** to remove source ports from a mirroring group.

Syntax

mirroring-group *group-id* **mirroring-port** *interface-list* { **both** | **inbound** | **outbound** }

undo mirroring-group *group-id* **mirroring-port** *interface-list*

Default

No source port is configured for a mirroring group.

Views

System view

Predefined user roles

network-admin

Parameters

group-id: Specifies a mirroring group by its ID. The value range for this argument is 1 to 4.

interface-list: Specifies a space-separated list of up to eight interface items. Each item specifies an interface by its type and number or specifies a range of interfaces in the form of *interface-type interface-number1* **to** *interface-type interface-number2*. When you specify a range of interfaces, the interfaces must be of the same type and on the same slot. The start interface number must be identical to or lower than the end interface number.

both: Mirrors both received and sent packets.

inbound: Mirrors only received packets.

outbound: Mirrors only sent packets.

Usage guidelines

You can configure source ports only for local mirroring groups and remote source groups.

A Layer 2 aggregate interface cannot be configured as a source port for a mirroring group.

Do not assign a source port of a mirroring group to the remote probe VLAN of the mirroring group.

The device supports only one mirroring group for outbound or bidirectional traffic mirroring.

A port can act as a source port for only one mirroring group.

A source port cannot be used as a reflector port, monitor port, or egress port.

Examples

Create local mirroring group 1 to monitor the bidirectional traffic of GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] mirroring-group 1 local
[Sysname] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 both
```

Create remote source group 2 to monitor the bidirectional traffic of GigabitEthernet 1/0/2.

```
<Sysname> system-view
[Sysname] mirroring-group 2 remote-source
[Sysname] mirroring-group 2 mirroring-port gigabitethernet 1/0/2 both
```

Related commands

mirroring-group

mirroring-group monitor-egress

Use **mirroring-group monitor-egress** to configure the egress port for a remote source group.

Use **undo mirroring-group monitor-egress** to restore the default.

Syntax

In system view:

mirroring-group *group-id* **monitor-egress** *interface-type interface-number*

undo mirroring-group *group-id* **monitor-egress** *interface-type interface-number*

In interface view:

mirroring-group *group-id* **monitor-egress**

undo mirroring-group *group-id* **monitor-egress**

Default

No egress port is configured for a remote source group.

Views

System view

Interface view

Predefined user roles

network-admin

Parameters

group-id: Specifies a mirroring group by its ID. The value range for this argument is 1 to 4.

interface-type interface-number: Specifies a port by its type and number.

Usage guidelines

You can configure egress ports only for remote source groups.

For port mirroring to work correctly, disable the following features on the egress port of a mirroring group:

- Spanning tree.
- 802.1X.
- IGMP snooping.
- Static ARP.
- MAC address learning.

The member port of an existing mirroring group cannot be configured as an egress port.

The member port of an aggregate interface cannot be configured as an egress port.

Examples

Create remote source group 1. Configure GigabitEthernet 1/0/1 as its egress port in system view.

```
<Sysname> system-view
[Sysname] mirroring-group 1 remote-source
[Sysname] mirroring-group 1 monitor-egress gigabitethernet 1/0/1
```

Create remote source group 2. Configure GigabitEthernet 1/0/2 as its egress port in interface view.

```
<Sysname> system-view
[Sysname] mirroring-group 2 remote-source
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] mirroring-group 2 monitor-egress
```

Related commands

mirroring-group

mirroring-group monitor-port (interface view)

Use **mirroring-group monitor-port** to configure a port as the monitor port for a mirroring group.

Use **undo mirroring-group monitor-port** to restore the default.

Syntax

mirroring-group *group-id* **monitor-port**

undo mirroring-group *group-id* **monitor-port**

Default

A port does not act as the monitor port for any mirroring groups.

Views

Interface view

Predefined user roles

network-admin

Parameters

group-id: Specifies a mirroring group by its ID. The value range for this argument is 1 to 4.

Usage guidelines

You can configure monitor ports only for local mirroring groups and remote destination groups.

Do not enable the spanning tree feature on the monitor port of a mirroring group.

For an aggregate interface configured as the monitor port of a mirroring group, do not configure its member ports as source ports of the mirroring group.

Use a monitor port only for port mirroring, so the data monitoring device receives and analyzes only the mirrored traffic.

The member port of an existing mirroring group cannot be configured as a monitor port.

The member port of an aggregate interface cannot be configured as a monitor port.

Only one monitor port can be configured for a mirroring group.

Examples

Create local mirroring group 1 and configure GigabitEthernet 1/0/1 as its monitor port.

```
<Sysname> system-view
[Sysname] mirroring-group 1 local
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mirroring-group 1 monitor-port
```

Create remote destination group 2 and configure GigabitEthernet 1/0/2 as its monitor port.

```
<Sysname> system-view
[Sysname] mirroring-group 2 remote-destination
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] mirroring-group 2 monitor-port
```

Related commands

mirroring-group

mirroring-group monitor-port (system view)

Use **mirroring-group monitor-port** to configure the monitor ports for a mirroring group.

Use **undo mirroring-group monitor-port** to remove the monitor ports from a mirroring group.

Syntax

mirroring-group *group-id* **monitor-port** *interface-type interface-number*

undo mirroring-group *group-id* **monitor-port** *interface-type interface-number*

Default

No monitor port is configured for a mirroring group.

Views

System view

Predefined user roles

network-admin

Parameters

group-id: Specifies a mirroring group by its ID. The value range for this argument is 1 to 4.

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

You can configure monitor ports only for local mirroring groups and remote destination groups.

Do not enable the spanning tree feature on the monitor port of a mirroring group.

For an aggregate interface configured as the monitor port of a mirroring group, do not configure its member ports as source ports of the mirroring group.

Use a monitor port only for port mirroring, so the data monitoring device receives only the mirrored traffic.

The member port of an existing mirroring group cannot be configured as a monitor port.

The member port of an aggregate interface cannot be configured as a monitor port.

Only one monitor port can be configured for a mirroring group.

Examples

Create local mirroring group 1 and configure GigabitEthernet 1/0/1 as its monitor port.

```
<Sysname> system-view
[Sysname] mirroring-group 1 local
[Sysname] mirroring-group 1 monitor-port gigabitethernet 1/0/1
```

Create remote destination group 2 and configure GigabitEthernet 1/0/2 as its monitor port.

```
<Sysname> system-view
[Sysname] mirroring-group 2 remote-destination
[Sysname] mirroring-group 2 monitor-port gigabitethernet 1/0/2
```

Related commands

mirroring-group

mirroring-group reflector-port

Use **mirroring-group reflector-port** to configure the reflector port for a remote source group.

Use **undo mirroring-group reflector-port** to restore the default.

Syntax

In system view:

mirroring-group *group-id* **reflector-port** *interface-type interface-number*

undo mirroring-group *group-id* **reflector-port** *interface-type interface-number*

In interface view:

mirroring-group *group-id* **reflector-port**

undo mirroring-group *group-id* **reflector-port**

Default

No reflector port is configured for a mirroring group.

Views

System view

Interface view

Predefined user roles

network-admin

Parameters

group-id: Specifies a mirroring group by its ID. The value range for this argument is 1 to 4.

interface-type interface-number: Specifies a port by its type and number.

Usage guidelines

CAUTION:

- The port to be configured as a reflector port must be a port not in use. Do not connect a network cable to a reflector port.
- When a port is configured as a reflector port, the port restores to the factory default settings. You cannot configure other features on a reflector port.
- If an IRF port is bound to only one physical interface, do not configure the physical interface as a reflector port. Otherwise, the IRF might split.

You can configure reflector ports only for remote source groups.

You cannot change the duplex mode, MDI settings, or speed for a reflector port.

The member port of an aggregate interface cannot be configured as a reflector port.

Examples

Create remote source group 1. Configure GigabitEthernet 1/0/1 as its reflector port in system view.

```
<Sysname> system-view
[Sysname] mirroring-group 1 remote-source
[Sysname] mirroring-group 1 reflector-port gigabitethernet 1/0/1
This operation may delete all settings made on the interface. Continue? [Y/N]: y
```

Create remote source group 2. Configure GigabitEthernet 1/0/2 as its reflector port in interface view.

```
<Sysname> system-view
[Sysname] mirroring-group 2 remote-source
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] mirroring-group 2 reflector-port
This operation may delete all settings made on the interface. Continue? [Y/N]: y
```

Related commands

mirroring-group

mirroring-group remote-probe vlan

Use **mirroring-group remote-probe vlan** to specify a VLAN as the remote probe VLAN for a mirroring group.

Use **undo mirroring-group remote-probe vlan** to restore the default.

Syntax

mirroring-group *group-id* **remote-probe vlan** *vlan-id*

undo mirroring-group *group-id* **remote-probe vlan** *vlan-id*

Default

No remote probe VLAN is configured for a mirroring group.

Views

System view

Predefined user roles

network-admin

Parameters

group-id: Specifies a mirroring group by its ID. The value range for this argument is 1 to 4.

vlan-id: Specifies a VLAN by its ID.

Usage guidelines

You can configure remote probe VLANs only for remote source groups and remote destination groups.

When a VLAN is configured as a remote probe VLAN, use the VLAN for port mirroring exclusively.

The remote mirroring groups on the source device and destination device must use the same remote probe VLAN.

Only a static VLAN that already exists can be configured as a remote probe VLAN. A VLAN can be configured as the remote probe VLAN for only one mirroring group.

To delete a VLAN that is configured as a remote probe VLAN, remove the remote probe VLAN configuration first.

The device supports only one remote probe VLAN.

Examples

Create remote source group 1 and configure VLAN 10 as its remote probe VLAN.

```
<Sysname> system-view
[Sysname] mirroring-group 1 remote-source
[Sysname] mirroring-group 1 remote-probe vlan 10
```

Create remote destination group 2 and configure VLAN 20 as its remote probe VLAN.

```
<Sysname> system-view
[Sysname] mirroring-group 2 remote-destination
[Sysname] mirroring-group 2 remote-probe vlan 20
```

Related commands

mirroring-group

Flow mirroring commands

mirror-to cpu

Use **mirror-to cpu** to configure a mirroring action that mirrors traffic to the CPU.

Use **undo mirror-to cpu** to delete the mirroring action that mirrors traffic to the CPU.

Syntax

mirror-to cpu

undo mirror-to cpu

Default

No mirroring action exists to mirror traffic to the CPU.

Views

Traffic behavior view

Predefined user roles

network-admin

Examples

Create traffic behavior 1 and configure the action of mirroring traffic to the CPU for the traffic behavior.

```
<Sysname> system-view
[Sysname] traffic behavior 1
[Sysname-behavior-1] mirror-to cpu
```

mirror-to interface

Use **mirror-to interface** to configure a mirroring action that mirrors traffic to an interface.

Use **undo mirror-to interface** to delete a mirroring action that mirrors traffic to an interface.

Syntax

mirror-to interface *interface-type interface-number*

undo mirror-to interface *interface-type interface-number*

Default

No mirroring actions exist to mirror traffic to interfaces.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

*interface-type interface-numbe*r: Specifies an interface by its type and number.

Usage guidelines

You can execute the **mirror-to interface** *interface-type interface-number* command multiple times for a traffic behavior to mirror traffic to different interfaces.

You can configure a maximum of four traffic behaviors that contain mirroring actions. If you configure more than four such traffic behaviors, only the first four traffic behaviors take effect.

You can use the **mirror-to interface** *interface-type interface-number* command to mirror traffic to only one interface in a traffic behavior. If you execute the command for a traffic behavior multiple times, the most recent configuration takes effect.

Examples

Create traffic behavior 1 and configure the action of mirroring traffic to GigabitEthernet 1/0/1 for the traffic behavior.

```
<Sysname> system-view
[Sysname] traffic behavior 1
[Sysname-behavior-1] mirror-to interface gigabitethernet 1/0/1
```

Contents

sFlow commands

display sflow

Use **display sflow** to display sFlow configuration and operation information.

Syntax

display sflow

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display sFlow configuration and operation information.

```
<Sysname> display sflow
sFlow datagram version: 5
Global information:
Agent IP: 10.10.10.1(CLI)
Source address: 10.0.0.1 2001::1
Collector information:
ID    IP              Port  Aging      Size VPN-instance Description
1     22:2:20::10     6535  N/A        1400              netserver
2     192.168.3.5     6543  500        1400              Office
Port counter sampling information:
Interface   Instance   CID   Interval(s)
GE1/0/1     2          2     100
GE1/0/1     1          1     200
Port flow sampling information:
Interface   Instance   FID   MaxHLen Rate       Mode      Status
GE1/0/1     2          2     128     1000       Random    Active
GE1/0/1     1          1     128     1000       Random    Active
```

Table 1 Command output

Field	Description
sFlow datagram version	sFlow version, which can only take the value of 5. The device can send only sFlow packets whose sFlow version is 5.
Global information	Global sFlow information.
Agent IP	IP address of the sFlow agent: • **CLI**—Manually configured IP address. • **Auto**—Automatically configured IP address.
Source address	Source IP address of sFlow packets.
Collector information	sFlow collector information.
ID	sFlow collector ID.

Field	Description
IP	sFlow collector IP address.
Port	sFlow collector port.
Aging	Remaining lifetime of the sFlow collector. If this field displays **N/A**, the sFlow collector never ages out.
Size	Maximum length of the sFlow data portion in an sFlow packet.
VPN-instance	This field is not supported in the current software version. Name of the VPN instance to which the sFlow collector belongs.
Description	Description of the sFlow collector.
Port counter sampling information	Information about interfaces configured with counter sampling.
Port flow sampling information	Information about interfaces configured with flow sampling.
Interface	Interface configured with sFlow.
Instance	ID of the sFlow instance for sending counter or flow sampled packets.
CID	ID of the sFlow collector for receiving counter sampled packets. If no sFlow collector ID is specified, this field displays **0**.
Interval(s)	Counter sampling interval, in seconds.
FID	ID of the sFlow collector for receiving flow sampled packets. If no sFlow collector ID is specified, this field displays **0**.
MaxHLen	Maximum number of bytes that can be copied in a sampled packet (starting from the packet header).
Rate	Number of packets out of which the interface samples a packet by using flow sampling.
Mode	Flow sampling mode.
Status	sFlow status of the port: • **Suspended**—The sFlow feature is suspended because the port is down. • **Active**—The sFlow feature is active because the port is up.

sflow agent

Use **sflow agent** to configure an IP address for the sFlow agent.

Use **undo sflow agent** to restore the default.

Syntax

sflow agent { **ip** *ipv4-address* | **ipv6** *ipv6-address* }

undo sflow agent { **ip** | **ipv6** }

Default

No IP address is configured for the sFlow agent. The device periodically identifies whether the sFlow agent has an IP address. If the sFlow agent does not have an IP address, the device automatically selects an IPv4 address for the sFlow agent. It does not save the IPv4 address in the configuration file.

Views

System view

Predefined user roles

network-admin

Parameters

ip *ipv4-address*: Specifies an IPv4 address for the sFlow agent.

ipv6 *ipv6-address*: Specifies an IPv6 address for the sFlow agent.

Usage guidelines

As a best practice, manually configure an IP address for the sFlow agent.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify IP address 10.10.10.1 for the sFlow agent.

```
<Sysname> system-view
[Sysname] sflow agent ip 10.10.10.1
```

sflow collector

Use **sflow collector** to configure parameters for an sFlow collector.

Use **undo sflow collector** to remove an sFlow collector.

Syntax

sflow collector *collector-id* { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**port** *port-number* | **datagram-size** *size* | **time-out** *seconds* | **description** *string*] *

undo sflow collector *collector-id*

Default

No sFlow collector information is configured.

Views

System view

Predefined user roles

network-admin

Parameters

collector-id: Specifies an sFlow collector by its ID. The value range for this argument is 1 to 10.

ip *ipv4-address*: Specifies an IPv4 address for the sFlow collector.

ipv6 *ipv6-address*: Specifies an IPv6 address for the sFlow collector.

port *port-number*: Specifies the UDP port number of the sFlow collector, in the range of 1 to 65535. The default is 6343.

datagram-size *size*: Specifies the maximum length of the sFlow data portion in an sFlow packet. The value range for the *size* argument is 200 to 3000 bytes, and the default value is 1400 bytes.

time-out *seconds*: Specifies the aging timer of the sFlow collector, in the range of 1 to 2147483647 seconds. When the aging timer expires, the sFlow collector settings are deleted. The sFlow collector settings do not age out by default.

description *string*: Specifies a description, a case-sensitive string of 1 to 127 characters. The default description is "CLI Collector."

Examples

Configure the following parameters for sFlow collector 2:

- **IP address**—3.3.3.1.
- **Port number**—Default.
- **Description**—netserver.
- **Aging timer**—1200 seconds.
- **Maximum length of the sFlow data portion in the sFlow packet**—1000 bytes.

```
<Sysname> system-view
[Sysname] sflow collector 2 ip 3.3.3.1 description netserver time-out 1200 datagram-size
1000
```

sflow counter collector

Use **sflow counter collector** to specify an sFlow instance and an sFlow collector for counter sampling.

Use **undo sflow counter collector** to restore the default.

Syntax

sflow counter [**instance** *instance-id*] **collector** *collector-id*

undo sflow counter [**instance** *instance-id*] **collector**

Default

No sFlow instance or sFlow collector is specified for counter sampling.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

instance *instance-id*: Specifies an sFlow instance by its ID in the range of 1 to 4. The default ID for an sFlow instance is 1. If you do not specify an sFlow instance, this command specifies sFlow instance 1 for counter sampling.

collector-id: Specifies an sFlow collector by its ID. The value range for this argument is 1 to 10.

Usage guidelines

This command enables the device to send counter sampling information on an interface to the specified sFlow collector.

On an interface, one sFlow instance has only one sFlow collector. To specify multiple sFlow collectors for counter sampling, execute this command multiple times and use different sFlow instances each time. If you execute this command multiple times but use the same sFlow instance and different sFlow collectors each time, the most recent configuration takes effect.

On an interface, counter sampling and flow sampling are separate from each other. They can have the same sFlow instance but different sFlow collectors specified.

Settings of sFlow instances and sFlow collectors for different interfaces do not affect each other. Configure this command based on actual requirement.

Examples

Specify sFlow instance 2 and sFlow collector 2 on GigabitEthernet 1/0/1 for counter sampling.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] sflow counter instance 2 collector 2
```

sflow counter interval

Use **sflow counter interval** to enable counter sampling and set a counter sampling interval.

Use **undo sflow counter interval** to disable counter sampling.

Syntax

sflow counter interval *interval*

undo sflow counter interval

Default

Counter sampling is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

interval: Specifies the counter sampling interval in the range of 2 to 86400 seconds.

Examples

Enable counter sampling and set the counter sampling interval to 120 seconds on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] sflow counter interval 120
```

sflow flow collector

Use **sflow flow collector** to specify an sFlow instance and an sFlow collector for flow sampling.

Use **undo sflow flow collector** to restore the default.

Syntax

sflow flow [**instance** *instance-id*] **collector** *collector-id*

undo sflow flow [**instance** *instance-id*] **collector**

Default

No sFlow instance or sFlow collector is specified for flow sampling.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

instance *instance-id*: Specifies an sFlow instance by its ID in the range of 1 to 4. The default ID for an sFlow instance is 1. If you do not specify an sFlow instance, this command specifies sFlow instance 1 for flow sampling.

collector-id: Specifies an sFlow collector by its ID. The value range for this argument is 1 to 10.

Usage guidelines

This command enables the device to send flow sampling information on an interface to the specified sFlow collector.

On an interface, one sFlow instance has only one sFlow collector. To specify multiple sFlow collectors for flow sampling, execute this command multiple times and use different sFlow instances each time. If you execute this command multiple times but use the same sFlow instance and different sFlow collectors each time, the most recent configuration takes effect.

On an interface, counter sampling and flow sampling are separate from each other. They can have the same sFlow instance but different sFlow collectors specified.

Settings of sFlow instances and sFlow collectors for different interfaces do not affect each other. Configure this command based on actual requirement.

Examples

Specify sFlow instance 2 and sFlow collector 2 on GigabitEthernet 1/0/1 for flow sampling.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] sflow flow instance 2 collector 2
```

sflow flow max-header

Use **sflow flow max-header** to set the maximum number of bytes (starting from the packet header) that flow sampling can copy per packet.

Use **undo sflow flow max-header** to restore the default.

Syntax

sflow flow max-header *length*

undo sflow flow max-header

Default

Flow sampling can copy up to 128 bytes of a packet.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

length: Specifies the maximum number of bytes that can be copied, in the range of 18 to 512. As a best practice, use the default value.

Examples

Set the maximum number of bytes to 60 for flow sampling to copy per packet on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] sflow flow max-header 60
```

sflow sampling-mode

Use **sflow sampling-mode** to specify a flow sampling mode.

Use **undo sflow sampling-mode** to restore the default.

Syntax

sflow sampling-mode random

undo sflow sampling-mode

Default

Random sampling is used.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

random: Specifies the random sampling mode. For example, if the packet sampling interval is set to 4000 (by using the **sflow sampling-rate** command), the device samples packets randomly as follows:

- The device might sample one packet from the first 4000 packets.
- The device might sample multiple packets from the next 4000 packets.
- The device might sample no packets from the third 4000 packets.

However, the device samples one packet from 4000 packets on average.

Examples

Specify random flow sampling mode on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] sflow sampling-mode random
```

Related commands

sflow sampling-rate

sflow sampling-rate

Use **sflow sampling-rate** to enable flow sampling and specify the number of packets out of which flow sampling will sample a packet.

Use **undo sflow sampling-rate** to disable flow sampling.

Syntax

sflow sampling-rate *rate*

undo sflow sampling-rate

Default

Flow sampling is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

rate: Specifies the number of packets out of which flow sampling will sample a packet on the interface. The value range for this argument is 1000 to 500000. As a best practice, set the sampling interval to 2^n that is greater than or equal to 8192, for example, 32768.

Examples

Enable flow sampling to sample a packet out of 32768 packets on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] sflow sampling-rate 32768
```

Related commands

sflow sampling-mode

sflow source

Use **sflow source** to specify the source IP address of sent sFlow packets.

Use **undo sflow source** to restore the default.

Syntax

sflow source { **ip** *ipv4-address* | **ipv6** *ipv6-address* } *

undo sflow source { **ip** | **ipv6** } *

Default

The source IP address of sent sFlow packets is determined by routing.

Views

System view

Predefined user roles

network-admin

Parameters

ip *ipv4-address*: Specifies the source IPv4 address of sent sFlow packets.

ipv6 *ipv6-address*: Specifies the source IPv6 address of sent sFlow packets.

Examples

Specify the source IPv4 address of sent sFlow packets as 10.0.0.1.

```
<Sysname> system-view
[Sysname] sflow source ip 10.0.0.1
```

Contents

Information center commands

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

diagnostic-logfile save

Use **diagnostic-logfile save** to manually save diagnostic logs from the diagnostic log file buffer to the diagnostic log file.

Syntax

diagnostic-logfile save

Views

Any view

Predefined user roles

network-admin

Usage guidelines

You can specify the directory to save the diagnostic log file by using the **info-center diagnostic-logfile directory** command.

The system clears the diagnostic log file buffer after saving the buffered diagnostic logs to the diagnostic log file.

If the diagnostic log file buffer is empty, this command displays a success message event though no logs are saved to the diagnostic log file.

Examples

Manually save diagnostic logs from the diagnostic log file buffer to the diagnostic log file.

```
<Sysname> diagnostic-logfile save
The contents in the diagnostic log file buffer have been saved to the file
flash:/diagfile/diagfile.log.
```

Related commands

info-center diagnostic-logfile enable

info-center diagnostic-logfile directory

display diagnostic-logfile summary

Use **display diagnostic-logfile summary** to display the diagnostic log file configuration.

Syntax

display diagnostic-logfile summary

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the diagnostic log file configuration.

```
<Sysname> display diagnostic-logfile summary
  Diagnostic log file: Enabled.
  Diagnostic log file size quota: 10 MB
  Diagnostic log file directory: flash:/diagfile
  Writing frequency: 24 hour 0 min 0 sec
```

Table 1 Command output

Field	Description
Diagnostic log file	Status of the diagnostic log file: • **Enabled**—Diagnostic logs can be output to the diagnostic log file. • **Disabled**—Diagnostic logs cannot be output to the diagnostic log file.
Diagnostic log file size quota	Maximum size for the diagnostic log file, in MB.
Log file directory	Directory where the diagnostic log file is saved.
Writing frequency	Interval at which the system saves diagnostic logs from the buffer to the diagnostic log file.

display info-center

Use **`display info-center`** to display information center configuration.

Syntax

`display info-center`

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display information center configuration.

```
<Sysname> display info-center
Information Center: Enabled
Console: Enabled
Monitor: Enabled
Log host: Enabled
    192.168.0.1, log output filter: loghost1,
    port number: 5000, host facility: local7
Log buffer: Enabled
    Max buffer size 1024, current buffer size 512,
    Current messages 0, dropped messages 0, overwritten messages 0
Log file: Enabled
Security log file: Enabled
Information timestamp format:
```

```
Log host: Date
Other output destination: Date
```

display info-center filter

Use **display info-center filter** to display information about log output filters.

Syntax

display info-center filter [*filter-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

filter-name: Specifies an existing log output filter by its name. If you do not specify a log output filter, this command displays information about all log output filters.

Examples

Display information about log output filter **loghost1**.

```
<Sysname> display info-center filter loghost1
 Log output filter: loghost1
 Module                        Rule
 ARP                           Debugging
 CFGLOG                        Deny
 Default                       Informational
```

Table 2 Command output

Field	Description
Log output filter:	Name of the log output filter.
Module	Module to which the log output filter applies.
Rule	Rules in the log output filter.

Related commands

info-center filter

display logbuffer

Use **display logbuffer** to display log buffer information and buffered logs.

Syntax

display logbuffer [**reverse**] [**level** *severity* | **size** *buffersize* | **slot** *slot-number*]* [**last-mins** *mins*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

reverse: Displays log entries chronologically, with the most recent entry at the top. If you do not specify this keyword, the command displays log entries chronologically, with the oldest entry at the top.

level *severity*: Specifies a severity level in the range of 0 to 7. If you do not specify a severity level, this command displays log information for all levels.

Table 3 Log levels

Severity value	Level	Description	Keyword in commands
0	Emergency	The system is unusable. For example, the system authorization has expired.	**emergency**
1	Alert	Action must be taken immediately. For example, traffic on an interface exceeds the upper limit.	**alert**
2	Critical	Critical condition. For example, the device temperature exceeds the upper limit, the power module fails, or the fan tray fails.	**critical**
3	Error	Error condition. For example, the link state changes.	**error**
4	Warning	Warning condition. For example, an interface is disconnected, or the memory resources are used up.	**warning**
5	Notification	Normal but significant condition. For example, a terminal logs in to the device, or the device reboots.	**notification**
6	Informational	Informational message. For example, a command or a **ping** operation is executed.	**informational**
7	Debugging	Debugging message.	**debugging**

size *buffersize*: Specifies the number of latest logs to be displayed. The value range is 1 to 1024. If you do not specify this option, the command displays all logs in the log buffer.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices.

last-mins *mins*: Displays logs buffered over the last specified period of time. The *mins* argument specifies a time period in the range of 1 to 43200 minutes. If you do not specify a time period, the command displays all logs in the log buffer.

Examples

Display log buffer information and buffered logs.

```
<Sysname> display logbuffer
Log buffer: Enabled
Max buffer size: 1024
Actual buffer size: 512
Dropped messages: 0
Overwritten messages: 718
Current messages: 512
%Jun 17 15:57:09:578 2016 Sysname SYSLOG/7/SYS_RESTART:System restarted --
```

```
...
```

Display log buffer information and logs buffered over the last 5 minutes.

```
<Sysname> display logbuffer last-mins 5
Log buffer: Enabled
Max buffer size: 1024
Actual buffer size: 512
Dropped messages: 0
Overwritten messages: 0
Current messages: 191
%Jan  1 01:00:06:784 2011 Sysname SHELL/6/SHELL_CMD:
-Line=vty0-IPAddr=192.168.1.242-User=**; Command is display current-configuration
%Jan  1 01:03:19:691 2018 Sysname SHELL/5/SHELL_LOGIN: VTY logged in from 192.168.1.33.
%Jan  1 01:03:21:269 2018 Sysname SHELL/6/SHELL_CMD:
-Line=vty1-IPAddr=192.168.1.33-User=**; Command is display logbuffer last-mins 5
```

Table 4 Command output

Field	Description
Log buffer	Status of the log buffer: • **Enabled**—Logs can be output to the log buffer. • **Disabled**—Logs cannot be output to the buffer.
Max buffer size	Maximum buffer size supported by the device.
Actual buffer size	Maximum buffer size configured by using the **info-center logbuffer size** command.
Dropped messages	Number of dropped messages.
Overwritten messages	Number of overwritten messages.
Current messages	Number of current messages.

Related commands

info-center logbuffer

reset logbuffer

display logbuffer summary

Use **display logbuffer summary** to display the log buffer summary.

Syntax

display logbuffer summary [**level** *severity* | **slot** *slot-number*] *

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

level *severity*: Specifies a severity level in the range of 0 to 7. If you do not specify a severity level, this command displays log information of all levels in the log buffer. For more information about log levels, see Table 3.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices.

Examples

Display the summary of the log buffer.

```
<Sysname> display logbuffer summary
  Slot EMERG ALERT  CRIT ERROR  WARN NOTIF  INFO DEBUG
     1     0     0     0     7     0    34    38     0
```

Table 5 Command output

Field	Description
EMERG	Represents emergency. For more information, see Table 3.
ALERT	Represents alert. For more information, see Table 3.
CRIT	Represents critical. For more information, see Table 3.
ERROR	Represents error. For more information, see Table 3.
WARN	Represents warning. For more information, see Table 3.
NOTIF	Represents notification. For more information, see Table 3.
INFO	Represents informational. For more information, see Table 3.
DEBUG	Represents debug. For more information, see Table 3.

display logfile buffer

Use **display logfile buffer** to display the content of the log file buffer.

Syntax

display logfile buffer

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

The system saves logs to the log file buffer before the logs are saved to the log file automatically or manually.

After saving the buffered logs to the log file, the system clears the log file buffer.

Examples

Display the content of the log file buffer.

```
<Sysname> display logfile buffer
%@356%Dec 13 16:53:45:495 2017 H3C SHELL/6/SHELL_CMD: -Line=con0-IPAddr=**-User=**;
Command is logfile save.
```

Related commands

info-center logfile frequency

logfile save

display logfile summary

Use **display logfile summary** to display the log file configuration.

Syntax

display logfile summary

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the log file configuration.

```
<Sysname> display logfile summary
  Log file: Enabled.
  Log file size quota: 2 MB
  Log file directory: flash:/logfile
  Writing frequency: 24 hour 0 min 10 sec
```

Table 6 Command output

Field	Description
Log file	Log file status: • **Enabled**—Logs can be output to the log file. • **Disabled**—Logs cannot be output to the log file.
Log file size quota	Maximum log file size, in MB.
Log file directory	Log file directory.
Writing frequency	Log file writing frequency.

display security-logfile buffer

Use **display security-logfile buffer** to display the content of the security log file buffer.

Syntax

display security-logfile buffer

Views

Any view

Predefined user roles

security-audit

Usage guidelines

The system saves security logs to the security log file buffer before the logs are saved to the security log file automatically or manually.

After saving the buffered security logs to the security log file, the system clears the security log file buffer.

To use this command, a local user must have the security-audit user role. For information about configuring the security-audit user role, see AAA commands in *Security Command Reference*.

Examples

Display the content of the security log file buffer.

```
<Sysname> display security-logfile buffer
%@1%Sep 17 11:13:16:609 2017 Sysname SHELL/5/SHELL_LOGIN: Console logged in from con0.
```

Related commands

`info-center security-logfile frequency`

`security-logfile save`

display security-logfile summary

Use **`display security-logfile summary`** to display the summary of the security log file.

Syntax

`display security-logfile summary`

Views

Any view

Predefined user roles

security-audit

Usage guidelines

To use this command, a local user must have the security-audit user role. For information about configuring the security-audit user role, see AAA commands in *Security Command Reference*.

Examples

Display the summary of the security log file.

```
<Sysname> display security-logfile summary
  Security log file: Enabled
  Security log file size quota: 10 MB
  Security log file directory: flash:/seclog
  Alarm threshold: 80%
  Current usage: 30%
  Writing frequency: 24 hour 0 min 0 sec
```

Table 7 Command output

Field	Description
Security log file	Status of the security log file: • **Enabled**—Security logs can be output to the security log file. • **Disabled**—Security logs cannot be output to the security log file.
Security log file size quota	Maximum storage space reserved for the security log file.

Field	Description
Security log file directory	Security log file directory.
Alarm-threshold	Alarm threshold of the security log file usage.
Current usage	Current usage of the security log file.
Writing frequency	Security log file writing frequency.

Related commands

authorization-attribute (*Security Command Reference*)

enable log updown

Use **enable log updown** to enable an interface to generate link up or link down logs when the interface state changes.

Use **undo enable log updown** to disable an interface from generating link up or link down logs when the interface state changes.

Syntax

enable log updown

undo enable log updown

Default

All interfaces are allowed to generate link up and link down logs.

Views

Interface view

Predefined user roles

network-admin

Examples

Disable GigabitEthernet 1/0/1 from generating link up or link down logs.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo enable log updown
```

info-center diagnostic-logfile directory

Use **info-center diagnostic-logfile directory** to configure the directory to save the diagnostic log file.

Syntax

info-center diagnostic-logfile directory *dir-name*

Default

The diagnostic log file directory is **flash:/diagfile**.

Views

System view

Predefined user roles

network-admin

Parameters

dir-name: Specifies a directory by its name, a string of 1 to 64 characters.

Usage guidelines

The specified directory must have been created.

This command cannot survive an IRF reboot or a master/subordinate switchover.

Examples

Set the diagnostic log file directory to **flash:/test**.

```
<Sysname> mkdir test
Creating directory flash:/test... Done.
<Sysname> system-view
[Sysname] info-center diagnostic-logfile directory flash:/test
```

info-center diagnostic-logfile enable

Use **info-center diagnostic-logfile enable** to enable saving diagnostic logs to the diagnostic log file.

Use **undo info-center diagnostic-logfile enable** to disable saving diagnostic logs to the diagnostic log file.

Syntax

info-center diagnostic-logfile enable

undo info-center diagnostic-logfile enable

Default

Saving diagnostic logs to the diagnostic log file is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command enables saving diagnostic logs to the diagnostic log file for centralized management. Users can view the diagnostic logs to monitor device activities and to troubleshoot problems.

Examples

Enable saving diagnostic logs to the diagnostic log file.

```
<Sysname> system-view
[Sysname] info-center diagnostic-logfile enable
```

info-center diagnostic-logfile frequency

Use **info-center diagnostic-logfile frequency** to configure the interval at which the system saves diagnostic logs from the diagnostic log file buffer to the diagnostic log file.

Use **undo info-center diagnostic-logfile frequency** to restore the default.

Syntax

info-center diagnostic-logfile frequency *freq-sec*

undo info-center diagnostic-logfile frequency

Default

The diagnostic log file saving interval is 86400 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

freq-sec: Specifies the diagnostic log file saving interval in seconds. The value range is 10 to 86400.

Usage guidelines

The system outputs diagnostic logs to the diagnostic log file buffer, and then saves the buffered logs to the diagnostic log file at the specified interval.

Examples

Set the diagnostic log file saving interval to 600 seconds.

```
<Sysname> system-view
[Sysname] info-center diagnostic-logfile frequency 600
```

Related commands

info-center diagnostic-logfile enable

info-center diagnostic-logfile quota

Use **info-center diagnostic-logfile quota** to set the maximum size for the diagnostic log file.

Use **undo info-center diagnostic-logfile quota** to restore the default.

Syntax

info-center diagnostic-logfile quota *size*

undo info-center diagnostic-logfile quota

Default

The maximum size for the diagnostic log file is 10 MB.

Views

System view

Predefined user roles

network-admin

Parameters

size: Specifies the maximum size for the diagnostic log file, in MB. The value range is 1 to 10.

Examples

Set the maximum size to 6 MB for the diagnostic log file.

```
<Sysname> system-view
```

```
[Sysname] info-center diagnostic-logfile quota 6
```

info-center enable

Use **info-center enable** to enable the information center.

Use **undo info-center enable** to disable the information center.

Syntax

info-center enable

undo info-center enable

Default

The information center is enabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable the information center.

```
<Sysname> system-view
[Sysname] info-center enable
Information center is enabled.
```

info-center filter

Use **info-center filter** to create a log output filter.

Syntax

info-center filter *filter-name* { *module-name* | **default** } { **deny** | **level** *severity* }

undo info-center filter *filter-name* [*module-name* | **default**]

Default

No log output filters exist.

Views

System view

Predefined user roles

network-admin

Parameters

filter-name: Specifies a name for the log output filter, a case-insensitive string of 1 to 8 characters.

module-name: Specifies a module by its name. To view the names of supported modules, execute the **info-center filter** *filter-name* **?** command.

default: Specifies all supported modules.

deny: Disables log output.

level *severity*: Specifies a log severity level by its name. Supported severity levels are **alert**, **critical**, **debugging**, **emergency**, **error**, **informational**, **notification**, and **warning**. See Table 3 for more information about the log severity levels. The log output filter applies to logs of the specified severity level and all higher levels.

Usage guidelines

A log output filter contains a set of log output filter rules for modules. You can use this command to create multiple log output filters. When specifying a log host, you can apply a log output filter to control log output to the log host.

You can also use the **info-center source** command to configure log output rules for the log host output destination. The system chooses the settings to control log output to a log host in the following order:

1. Log output filter specified for the log host by using the **info-center loghost** command.
2. Log output rules configured for the log host output destination by using the **info-center source** command.
3. Default log output rules (see Table 8).

Follow these restrictions and guidelines when you configure a log output filter:

- To set a log output filter rule for a module, use the *module-name* argument to specify the module name.

  If you set log output filter rules for the same module multiple times, the most recent configuration takes effect.
- To set a general log output filter rule for all modules, use the **default** keyword. The general log output filter rule applies to all modules that do not have module-specific filter rules.

  If you set a general log output filter rule multiple times, the most recent configuration takes effect.
- If no general log output filter rule is set, the system outputs logs with severity levels **informational** through **alert** for modules that do not have module-specific filter rules.
- To remove a module-specific log output filter rule, you must use the *module-name* argument. If you do not specify any parameters, the entire log output filter is deleted.

Examples

Create log output filter **loghost1**. In the log output filter, enable the ARP module to output logs with severity levels **notification** through **alert**, the SNMP module to output logs with severity levels **warning** through **alert**, and disable log output of all other modules.

```
<Sysname> system-view
[Sysname] info-center filter loghost1 arp level notification
[Sysname] info-center filter loghost1 snmp level warning
[Sysname] info-center filter loghost1 default deny
```

Related commands

display info-center filter

info-center loghost

info-center source

info-center format

Use **info-center format** to set the format for logs sent to log hosts.

Use **undo info-center format** to restore the default.

Syntax

info-center format { **cmcc** | **unicom** }

undo info-center format

Default

Logs are sent to log hosts in standard format.

Views

System view

Predefined user roles

network-admin

Parameters

cmcc: Specifies the China Mobile Communications Corporation (CMCC) format.

unicom: Specifies the China Unicom format.

Usage guidelines

Logs can be sent to log hosts in standard, China Unicom, or CMCC format. For more information about log formats, see *Network Management and Monitoring Configuration Guide*.

Examples

Set the log format to China Unicom for logs sent to log hosts.

```
<Sysname> system-view
[Sysname] info-center format unicom
```

info-center logbuffer

Use **info-center logbuffer** to enable log output to the log buffer.

Use **undo info-center logbuffer** to disable log output to the log buffer.

Syntax

info-center logbuffer

undo info-center logbuffer

Default

Log output to the log buffer is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command enables log output to log buffers based on the log source modules.

- Logs generated by modules that have separate log buffers are saved to their respective log buffers.

  For example, session logs are saved to the session log buffer.
- Logs generated by other modules are saved to the general log buffer.

To view log buffer information and buffered logs, use the **display logbuffer** command.

To set the log buffer size, use the **info-center logbuffer size** command.

Examples

Enable log output to the log buffer.

```
<Sysname> system-view
[Sysname] info-center logbuffer
```

Related commands

display logbuffer

info-center enable

info-center logbuffer size

Use **info-center logbuffer size** to set the maximum number of logs that can be buffered.

Use **undo info-center logbuffer size** to restore the default.

Syntax

info-center logbuffer size *buffersize*

undo info-center logbuffer size

Default

A maximum of 512 logs can be buffered.

Views

System view

Predefined user roles

network-admin

Parameters

buffersize: Specifies the maximum log buffer size. The value range is 0 to 1024.

Examples

Set the maximum log buffer size to 50.

```
<Sysname> system-view
[Sysname] info-center logbuffer size 50
```

Restore the default maximum log buffer size.

```
<Sysname> system-view
[Sysname] undo info-center logbuffer size
```

Related commands

display logbuffer

info-center enable

info-center logfile directory

Use **info-center logfile directory** to specify the directory to save the log file.

Syntax

info-center logfile directory *dir-name*

Default

The log file directory is **flash:/logfile**.

Views

System view

Predefined user roles

network-admin

Parameters

dir-name: Specifies a directory by its name, a string of 1 to 64 characters.

Usage guidelines

The specified log file directory must have been created.

The log file uses the .log extension.

This command cannot survive an IRF reboot or a master/subordinate switchover.

Examples

Set the log file directory to **flash:/test**.

```
<Sysname> mkdir test
Creating directory flash:/test... Done.
<Sysname> system-view
[Sysname] info-center logfile directory flash:/test
```

Related commands

info-center logfile enable

info-center logfile enable

Use **info-center logfile enable** to enable the log file feature.

Use **undo info-center logfile enable** to disable the log file feature.

Syntax

info-center logfile enable

undo info-center logfile enable

Default

The log file feature is enabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable log output to the log file.

```
<Sysname> system-view
[Sysname] info-center logfile enable
```

info-center logfile frequency

Use **info-center logfile frequency** to configure the interval at which the system saves logs from the log file buffer to the log file.

Use **undo info-center logfile frequency** to restore the default.

Syntax

info-center logfile frequency *freq-sec*

undo info-center logfile frequency

Default

The log file saving interval is 86400 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

freq-sec: Specifies the log file saving interval in seconds. The value range is 1 to 86400.

Usage guidelines

This command enables the system to automatically save logs in the log file buffer to the log file at the specified interval.

Examples

Set the log file saving interval to 60000 seconds.

```
<Sysname> system-view
[Sysname] info-center logfile frequency 60000
```

Related commands

info-center logfile enable

info-center logfile overwrite-protection

Use **info-center logfile overwrite-protection** to enable log file overwrite-protection.

Use **undo info-center logfile overwrite-protection** to disable log file overwrite-protection.

Syntax

info-center logfile overwrite-protection [**all-port-powerdown**]

undo info-center logfile overwrite-protection

Default

Log file overwrite-protection is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

all-port-powerdown: Shuts down all the service ports on the device when no log file space or storage device space is available. If you do not specify this keyword, the device does not shut down service ports when no log file space or storage device space is available.

Usage guidelines

This command is available only in FIPS mode.

Log file overwrite protection enables the system to stop saving new logs when no log file space or storage device space is available.

Examples

Enable log file overwrite-protection.

```
<Sysname> system-view
[Sysname] info-center logfile overwrite-protection
```

info-center logfile size-quota

Use **info-center logfile size-quota** to set the maximum log file size.

Use **undo info-center logfile size-quota** to restore the default.

Syntax

info-center logfile size-quota *size*

undo info-center logfile size-quota

Default

The maximum log file size is 10 MB.

Views

System view

Predefined user roles

network-admin

Parameters

size: Specifies the maximum log file size in MB. The value range is 1 to 10.

Examples

Set the maximum log file size to 2 MB.

```
<Sysname> system-view
[Sysname] info-center logfile size-quota 2
```

Related commands

info-center logfile enable

info-center logging suppress duplicates

Use **info-center logging suppress duplicates** to enable duplicate log suppression.

Use **undo info-center logging suppress duplicates** to disable duplicate log suppression.

Syntax

info-center logging suppress duplicates

undo info-center logging suppress duplicates

Default

Duplicate log suppression is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Outputting consecutive duplicate logs wastes system and network resources and increases device maintenance costs. You can enable this feature to suppress output of consecutive duplicate logs.

Examples

Enable duplicate log suppression on device A.

```
<Sysname> system-view
[Sysname] info-center logging suppress duplicates
```

info-center logging suppress module

Use **info-center logging suppress module** to configure a log suppression rule for a module.

Use **undo info-center logging suppress module** to delete a log suppression rule.

Syntax

info-center logging suppress module *module-name* **mnemonic** { **all** | *mnemonic-value* }

undo info-center logging suppress module *module-name* **mnemonic** { **all** | *mnemonic-value* }

Default

The device does not suppress output of any logs from any modules.

Views

System view

Predefined user roles

network-admin

Parameters

module-name: Specifies a log source module by its name, a case-insensitive string of 1 to 8 characters. To view the list of available log source modules, use the **info-center logging suppress module ?** command.

mnemonic { **all** | *mnemonic-value* }: Configures a mnemonic filter for log suppression.

- **all**: Suppresses output of all logs of the module.
- *mnemonic-value*: Suppresses output of logs with the specified mnemonic value. The *mnemonic-value* argument is a case-insensitive string of 1 to 32 characters, which must be the complete value contained in the mnemonic field of the log message. Log suppression will fail if a partial mnemonic value is specified.

Usage guidelines

You can configure log suppression rules to filter out the logs that you are not concerned with. A log suppression rule suppresses output of all logs or only logs with a specific mnemonic value for a module.

Examples

Configure a log suppression rule to suppress output of logs with the **shell_login** mnemonic value for the shell module.

```
<Sysname> system-view
[Sysname] info-center logging suppress module shell mnemonic shell_login
```

Related commands

info-center source

info-center loghost

Use **info-center loghost** to specify a log host and to configure output parameters.

Use **undo info-center loghost** to remove a log host.

Syntax

info-center loghost { *hostname* | *ipv4-address* | **ipv6** *ipv6-address* } [**port** *port-number*] [**dscp** *dscp-value*] [**facility** *local-number*] [**filter** *filter-name*]

undo info-center loghost { *hostname* | *ipv4-address* | **ipv6** *ipv6-address* }

Default

No log hosts are specified.

Views

System view

Predefined user roles

network-admin

Parameters

hostname: Specifies a log host by its name, a case-insensitive string of 1 to 253 characters. The host name can contain letters, digits, and special characters including hyphen (-), underscore (_), and dot (.).

ipv4-address: Specifies a log host by its IPv4 address.

ipv6 *ipv6-address*: Specifies a log host by its IPv6 address.

port *port-number*: Specifies the port number of the log host, in the range of 1 to 65535. The default is 514. It must be the same as the value configured on the log host. Otherwise, logs cannot be sent to the log host.

dscp *dscp-value*: Specifies the DSCP value in log packets sent to the log host. The value range for the *dscp-value* argument is 0 to 63, and the default is 0. The DSCP value of a packet defines the priority of the packet and affects the transmission priority of the packet. A greater DSCP value represents a higher priority.

facility *local-number*: Specifies a logging facility from local0 to local7 for the log host. The default value is local7. Logging facilities are used to mark different logging sources, and query and filer logs.

filter *filter-name*: Specifies a log output filter to control log output to the log host. The *filter-name* argument represents the filter name, a case-insensitive string of 1 to 8 characters. If you do not specify a log output filter, the log output rules configured by using the **info-center source** command for the log host destination are used.

Usage guidelines

The **info-center loghost** command takes effect only after the information center is enabled by using **info-center enable** command.

The device supports a maximum of 20 log hosts.

Examples

Output logs to the log host at 1.1.1.1.

```
<Sysname> system-view
[Sysname] info-center loghost 1.1.1.1
```

Related commands

info-center filter

info-center source

info-center loghost source

Use **info-center loghost source** to specify a source IP address for logs sent to log hosts.

Use **undo info-center loghost source** to restore the default.

Syntax

info-center loghost source *interface-type interface-number*

undo info-center loghost source

Default

The source IP address of logs sent to log hosts is the primary IP address of the outgoing interface.

Views

System view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

The system uses the primary IP address of the specified interface as the source IP address of the logs sent to log hosts.

The **info-center loghost source** command takes effect only after the information center is enabled by using **info-center enable** command.

Examples

Use the IP address of interface Loopback 0 as the source IP address of the logs sent to log hosts.

```
<Sysname> system-view
[Sysname] interface loopback 0
[Sysname-LoopBack0] ip address 2.2.2.2 32
[Sysname-LoopBack0] quit
```

```
[Sysname] info-center loghost source loopback 0
```

info-center security-logfile alarm-threshold

Use **info-center security-logfile alarm-threshold** to set the alarm threshold for security log file usage.

Use **undo info-center security-logfile alarm-threshold** to restore the default.

Syntax

info-center security-logfile alarm-threshold *usage*

undo info-center security-logfile alarm-threshold

Default

The alarm threshold for security log file usage is 80. When the usage of the security log file reaches 80%, the system outputs a message to inform the administrator.

Views

System view

Predefined user roles

network-admin

Parameters

usage: Specifies an alarm threshold. The value must be an integer in the range of 1 to 100.

Usage guidelines

When the security log file is full, the system deletes the oldest logs and then writes new logs to the security log file. This feature helps avoid security log loss by setting an alarm threshold for the security log file usage. When the threshold is reached, the system outputs log information to inform the administrator. The administrator can log in to the device with the security-audit user role and back up the security log file.

Examples

Set the alarm threshold for security log file usage to 90.

```
<Sysname> system-view
[Sysname] info-center security-logfile alarm-threshold 90
```

Related commands

info-center security-logfile size-quota

info-center security-logfile directory

Use **info-center security-logfile directory** to specify the security log file directory.

Syntax

info-center security-logfile directory *dir-name*

Default

The security log file is saved in the **flash:/seclog** directory.

Views

System view

Predefined user roles

security-audit

Parameters

dir-name: Specifies a directory by its name, a string of 1 to 64 characters.

Usage guidelines

The specified directory must have been created.

To use this command, a local user must have the security-audit user role. For information about configuring the security-audit user role, see AAA commands in *Security Command Reference.*

This command cannot survive an IRF reboot or a master/subordinate switchover.

Examples

Set the security log file directory to **flash:/test**.

```
<Sysname> mkdir test
Creating directory flash:/test... Done.
<Sysname> system-view
[Sysname] info-center security-logfile directory flash:/test
```

info-center security-logfile enable

Use **info-center security-logfile enable** to enable saving of security logs to the security log file.

Use **undo info-center security-logfile enable** to restore the default.

Syntax

info-center security-logfile enable

undo info-center security-logfile enable

Default

The saving of security logs to the security log file is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This feature enables the system to output security logs to the security log file buffer, and then saves the buffered logs to the security log file regularly.

Examples

Enable saving security logs to the security log file.

```
<Sysname> system-view
[Sysname] info-center security-logfile enable
```

info-center security-logfile frequency

Use **info-center security-logfile frequency** to configure the interval for saving security logs to the security log file.

Use **undo info-center security-logfile frequency** to restore the default.

Syntax

info-center security-logfile frequency *freq-sec*

undo info-center security-logfile frequency

Default

The security log file saving interval is 86400 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

freq-sec: Specifies the security log file saving interval in seconds. The value range is 10 to 86400 seconds.

Usage guidelines

The system outputs security logs to the security log file buffer, and then saves the buffered logs to the security log file at the specified interval.

Examples

Set the security log file saving interval to 600 seconds.

```
<Sysname> system-view
[Sysname] info-center security-logfile frequency 600
```

Related commands

info-center security-logfile enable

info-center security-logfile size-quota

Use **info-center security-logfile size-quota** to set the maximum size for the security log file.

Use **undo info-center security-logfile size-quota** to restore the default.

Syntax

info-center security-logfile size-quota *size*

undo info-center security-logfile size-quota

Default

The maximum size for the security log file is 10 MB.

Views

System view

Predefined user roles

network-admin

Parameters

size: Sets the maximum size for the security log file, in MB. The value range is 1 to 10.

Examples

Set the maximum size to 6 MB for the security log file.

```
<Sysname> system-view
[Sysname] info-center security-logfile size-quota 6
```

Related commands

info-center security-logfile alarm-threshold

info-center source

Use **info-center source** to configure a log output rule for a module.

Use **undo info-center source** to restore the default.

Syntax

info-center source { *module-name* | **default** } { **console** | **logbuffer** | **logfile** | **loghost** | **monitor** } { **deny** | **level** *severity* }

undo info-center source { *module-name* | **default** } { **console** | **logbuffer** | **logfile** | **loghost** | **monitor** }

Default

Table 8 lists the default log output rules.

Table 8 Default output rules

Destination	Log source modules	Output switch	Severity
Console	All supported modules	Enabled	Debug
Monitor terminal	All supported modules	Disabled	Debug
Log host	All supported modules	Enabled	Informational
Log buffer	All supported modules	Enabled	Informational
Log file	All supported modules	Enabled	Informational

Views

System view

Predefined user roles

network-admin

Parameters

module-name: Specifies a module by its name. You can use the **info-center source ?** command to view the modules supported by the device.

default: Specifies all supported modules.

console: Outputs logs to the console.

logbuffer: Outputs logs to the log buffer.

logfile: Outputs logs to the log file.

loghost: Outputs logs to the log host.

monitor: Outputs logs to the monitor terminal.

deny: Disables log output.

level *severity*: Specifies a severity level in the range of 0 to 7. The smaller the severity value, the higher the severity level. See Table 3 for more information. Logs at the specified severity level and higher levels are allowed or denied to be output.

Usage guidelines

If you do not set an output rule for a module, the module uses the output rule set by using the **default** keyword. If no rule is set by using the **default** keyword, the module uses the default output rule.

To modify or remove an output rule set for a module, you must use the *module-name* argument. A new output rule configured by using the **default** keyword does not take effect on the module.

If you execute this command for a module multiple times, the most recent configuration takes effect.

If you execute this command for the **default** modules multiple times, the most recent configuration takes effect.

Examples

Output only VLAN module's information with the emergency level to the console.

```
<Sysname> system-view
[Sysname] info-center source default console deny
[Sysname] info-center source vlan console level emergency
```

Based on the previous configuration, disable output of VLAN module's information to the console so no system information is output to the console.

```
<Sysname> system-view
[Sysname] undo info-center source vlan console
```

info-center synchronous

Use **info-center synchronous** to enable synchronous information output.

Use **undo info-center synchronous** to disable synchronous information output.

Syntax

info-center synchronous

undo info-center synchronous

Default

Synchronous information output is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

System log output interrupts ongoing configuration operations, including obscuring previously entered commands. Synchronous information output shows the obscured commands. It also provides a command prompt in command editing mode, or a [Y/N] string in interaction mode so you can continue your operation from where you were stopped.

Examples

Enable synchronous information output, and then execute the **display current-configuration** command to view the current configuration of the device.

```
<Sysname> system-view
[Sysname] info-center synchronous
Info-center synchronous output is on
[Sysname] display current-
```

At this time, the system receives log information. It displays the log information first, and then displays your previous input, which is **display current-** in this example.

```
%May 21 14:33:19:425 2007 Sysname SHELL/5/SHELL_LOGIN: VTY logged in from 192.168.1.44
[Sysname] display current-
```

Enter **configuration** to complete the **display current-configuration** command, and press the **Enter** key to execute the command.

Enable synchronous information output, and then save the current configuration (enter interactive information).

```
<Sysname> system-view
[Sysname] info-center synchronous
Info-center synchronous output is on
[Sysname] save
The current configuration will be written to the device. Are you sure? [Y/N]:
```

At this time, the system receives the log information. It displays the log information first and then displays [Y/N].

```
%May 21 14:33:19:425 2007 Sysname SHELL/5/SHELL_LOGIN: VTY logged in from 192.168.1.44
[Y/N]:
```

Enter **Y** or **N** to complete your input.

info-center syslog min-age

Use **info-center syslog min-age** to set the minimum storage period for logs in the log buffer and log file.

Use **undo info-center syslog min-age** to restore the default.

Syntax

info-center syslog min-age *min-age*

undo info-center syslog min-age

Default

The minimum storage period is not set.

Views

System view

Predefined user roles

network-admin

Parameters

min-age: Sets the minimum storage period in hours. The value range is 1 to 8760.

Examples

Set the minimum storage period to 168 hours.

```
<Sysname> system-view
[Sysname] info-center syslog min-age 168
```

info-center syslog trap buffersize

Use **info-center syslog trap buffersize** to set the maximum number of log traps that can be stored in the log trap buffer.

Use **undo info-center syslog trap buffersize** to restore the default.

Syntax

info-center syslog trap buffersize *buffersize*

undo info-center syslog trap buffersize

Default

The log trap buffer can store a maximum of 1024 traps.

Views

System view

Predefined user roles

network-admin

Parameters

buffersize: Specifies the maximum number of log traps that can be stored in the log trap buffer. The value range is 0 to 65535. Value 0 indicates that the device does not buffer log traps.

Usage guidelines

Log traps are SNMP notifications stored in the log trap buffer. After the **snmp-agent trap enable syslog** command is configured, the device sends log messages in SNMP notifications to the log trap buffer. You can view the log traps by accessing the MIB corresponding to the trap buffer.

The default buffer size is usually used. You can adjust the buffer size according to your network condition. New traps overwrite the oldest traps when the log trap buffer is full.

Examples

Set the log trap buffer size to 2048.

```
<Sysname> system-view
[Sysname] info-center syslog trap buffersize 2048
```

Related commands

snmp-agent trap enable syslog

info-center timestamp

Use **info-center timestamp** to set the timestamp format for logs sent to the console, monitor terminal, log buffer, and log file.

Use **undo info-center timestamp** to restore the default.

Syntax

info-center timestamp { **boot** | **date** | **none** }

undo info-center timestamp

Default

The timestamp format for logs sent to the console, monitor terminal, log buffer, and log file is **date**.

Views

System view

Predefined user roles

network-admin

Parameters

boot: Sets the timestamp format to xxx.yyy, where xxx is the most significant 32 bits (in milliseconds) and yyy is the least significant 32 bits. For example, 0.21990989 equals Jun 25 14:09:26:881 2007. The **boot** time shows the time since system startup.

date: Sets the timestamp format to MMM DD hh:mm:ss:ms YYYY, such as Dec 8 10:12:21:708 2007. The **date** time shows the current system time.

- MMM: Abbreviations of the months in English, which could be Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, or Dec.
- DD: Date, starting with a space if it is less than 10, for example " 7".
- hh:mm:ss:ms: Local time, with hh in the range of 00 to 23, mm and ss in the range of 00 to 59, and ms in the range of 0 to 999.
- YYYY: Year.

none: Indicates no time information is provided.

Examples

Set the timestamp format to **boot** for logs sent to the console, monitor terminal, log buffer, and log file.

```
<Sysname> system-view
[Sysname] info-center timestamp boot
```

Related commands

info-center timestamp loghost

info-center timestamp loghost

Use **info-center timestamp loghost** to set the timestamp format for logs sent to log hosts.

Use **undo info-center timestamp loghost** to restore the default.

Syntax

info-center timestamp loghost { **date** [**with-milliseconds**] | **iso** [**with-milliseconds** | **with-timezone**] * | **no-year-date** | **none** }

undo info-center timestamp loghost

Default

The timestamp format for logs sent to log hosts is **date**.

Views

System view

Predefined user roles

network-admin

Parameters

date: Sets the timestamp format to MMM DD hh:mm:ss YYYY, such as Dec 8 10:12:21 2007. The **date** time shows the current system time.

iso: Sets the ISO 8601 timestamp format, for example, 2009-09-21T15:32:55.

with-milliseconds: Sets the timestamp to be accurate to milliseconds for logs output to log hosts in date or ISO 8601 format. The millisecond value is appended to the time information in the timestamp with a dot as the separator. If you do not specify this keyword, the timestamp in date or ISO 8601 format is accurate to seconds.

- Example of a timestamp in date format with millisecond accuracy: Dec 8 10:12:21.708 2018.
- Example of a timestamp in ISO 8601 format with millisecond accuracy: 2018-09-21T15:32:55.708.

with-timezone: Includes the time zone information in the ISO format timestamp. For example, 2009-09-21T15:32:55+01:00. By default, the ISO format timestamp does not contain the time zone information.

no-year-date: Sets the timestamp format to the current system date and time without year or millisecond information.

none: Indicates that no timestamp information is provided.

Examples

Set the timestamp format to **no-year-date** for logs sent to log hosts.

```
<Sysname> system-view
[Sysname] info-center timestamp loghost no-year-date
```

Related commands

info-center timestamp

info-center trace-logfile quota

Use **info-center trace-logfile quota** to set the maximum size for the trace log file.

Use **undo info-center trace-logfile quota** to restore the default.

Syntax

info-center trace-logfile quota *size*

undo info-center trace-logfile quota

Default

The maximum size for the trace log file is 1 MB.

Views

System view

Predefined user roles

network-admin

Parameters

size: Sets the maximum size for the trace log file, in MB. The value range is 1 to 10.

Examples

Set the maximum size to 6 MB for the trace log file.

```
<Sysname> system-view
```

```
[Sysname] info-center trace-logfile quota 6
```

logfile save

Use **logfile save** to manually save logs in the log file buffer to the log file.

Syntax

logfile save

Views

Any view

Predefined user roles

network-admin

Usage guidelines

You can specify the directory to save the log file by using the **info-center logfile directory** command.

The system clears the log file buffer after saving the buffered logs to the log file automatically or manually.

If the log file buffer is empty, this command displays a success message event though no logs are saved to the log file.

Examples

Manually save logs from the log file buffer to the log file.

```
<Sysname> logfile save
The contents in the log file buffer have been saved to the file flash:/logfile/logfile.log.
```

Related commands

info-center logfile enable

info-center logfile directory

reset logbuffer

Use **reset logbuffer** to clear the log buffer.

Syntax

reset logbuffer

Views

User view

Predefined user roles

network-admin

Examples

Clear the log buffer.

```
<Sysname> reset logbuffer
```

Related commands

display logbuffer

security-logfile save

Use **security-logfile save** to manually save security logs from the security log file buffer to the security log file.

Syntax

security-logfile save

Views

Any view

Predefined user roles

security-audit

Usage guidelines

The system clears the security log file buffer after saving the buffered security logs to the security log file automatically or manually.

If the security log file buffer is empty, this command displays a success message event though no security logs are saved to the security log file.

To use this command, a local user must have the security-audit user role. For information about configuring the security-audit user role, see AAA commands in *Security Command Reference*.

Examples

Manually save the security logs in the security log file buffer to the security log file.

```
<Sysname> security-logfile save
The contents in the security log file buffer have been saved to the file
flash:/seclog/seclog.log.
```

Related commands

info-center security-logfile directory

authorization-attribute (*Security Command Reference*)

snmp-agent trap enable syslog

Use **snmp-agent trap enable syslog** to enable SNMP notifications for log messages.

Use **undo snmp-agent trap enable syslog** to disable SNMP notifications for log messages.

Syntax

snmp-agent trap enable syslog

undo snmp-agent trap enable syslog

Default

The device does not send SNMP notifications for log messages.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command enables the device to send an SNMP notification for each log message it outputs. The device encapsulates logs in SNMP notifications and then sends them to the SNMP module and the log trap buffer.

For the SNMP module to send the received SNMP notifications correctly, you must also configure SNMP on the device. For more information about SNMP configuration, see the network management and monitoring configuration guide for the device.

To view the traps in the log trap buffer, access the MIB corresponding to the log trap buffer. The log trap buffer size can be set by using the **info-center syslog trap buffersize** command.

Examples

Enable the device to send SNMP notifications for log messages.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable syslog
```

Related commands

info-center syslog trap buffersize

terminal debugging

Use **terminal debugging** to enable display of debug information on the current terminal.

Use **undo terminal debugging** to disable display of debug information on the current terminal.

Syntax

terminal debugging

undo terminal debugging

Default

Display of debug information is disabled on the current terminal.

Views

User view

Predefined user roles

network-admin

Usage guidelines

To enable display of debug information on the console, perform the following tasks:

1. Execute the **terminal debugging** command.
2. Enable the information center. The information center is enabled by default.
3. Use a debugging command to enable the related debugging.

To enable display of debug information on the current terminal, perform the following tasks:

1. Execute the **terminal monitor** and **terminal debugging** commands.
2. Enable the information center. The information center is enabled by default.
3. Use a debugging command to enable the related debugging.

This command takes effect only for the current connection between the terminal and the device. If a new connection is established, the default is restored.

You can also enable display of debug information on the current terminal by executing the **terminal logging level 7** command. This command has the following differences from the **terminal debugging** command:

- The **terminal logging level 7** command enables log display for all levels (levels **0** through **7**) on the current terminal.
- The **terminal debugging** command only enables display of logs with the following severity levels:
  - Debug level (level **7**).
  - Severity level higher than or equal to the level specified in the **terminal logging level** command.

Examples

Enable display of debug information on the current terminal.

```
<Sysname> terminal debugging
The current terminal is enabled to display debugging logs.
```

Related commands

terminal logging level

terminal monitor

terminal logging level

Use **terminal logging level** to set the lowest level of logs that can be output to the current terminal.

Use **undo terminal logging level** to restore the default.

Syntax

terminal logging level *severity*

undo terminal logging level

Default

The lowest level of logs that can be output to the current terminal is 6 (Informational).

Views

User view

Predefined user roles

network-admin

Parameters

severity: Specifies a log severity level. Valid values are alert, critical, debugging, emergency, error, informational, notification, warning, and digits from 0 to 7.

Usage guidelines

This command enables the device to output logs with a severity level higher than or equal to the specified level to the current terminal. For example, if you set the *severity* argument to 6, logs with a severity value from 0 to 6 are output to the current terminal.

This command takes effect only for the current connection between the terminal and the device. If a new connection is established, the default is restored.

Examples

Configure the device to output logs with the debugging level and higher levels to the current terminal.

```
<Sysname> terminal logging level 7
```

terminal monitor

Use **terminal monitor** to enable monitoring of logs on the current terminal.

Use **undo terminal monitor** to disable monitoring of logs on the current terminal.

Syntax

terminal monitor

undo terminal monitor

Default

Monitoring of logs is enabled on the console and disabled on the monitor terminal.

Views

User view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only for the current connection between the terminal and the device. If a new connection is established, the default is restored.

Examples

Enable monitoring of logs on the current terminal.

```
<Sysname> terminal monitor
The current terminal is enabled to display logs.
```

Contents

VCF fabric commands

The following switch series do not support VCF fabric:

- S5110V2-SI
- S5000V3-EI
- S5000V5-EI
- S5000E-X
- S5000X-EI
- S5120V2-LI
- S5130S-LI
- S5120V3-LI
- S5120V3-SI
- S3100V3-SI
- MS4320V2, MS4320, MS4200, MS4300V2, MS4320V3
- WS5810-WiNet, WS5820-WiNet
- WAS6000

display vcf-fabric role

Use **display vcf-fabric role** to display the role of the device in the VCF fabric.

Syntax

display vcf-fabric role

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

Use this command to display the default role and the current role of the device in the VCF fabric. To change the current role of the device, use the **vcf-fabric role** command.

Examples

Display the role of the device in the VCF fabric.

```
<System> display vcf-fabric role
Default role: access
Current role: access
```

Table 1 Command output

Field	Description
Default role	Default role of the device.
Current role	Current role of the device.

Related commands

vcf-fabric role

display vcf-fabric underlay autoconfigure

Use **display vcf-fabric underlay autoconfigure** to display information about automated underlay network deployment.

Syntax

display vcf-fabric underlay autoconfigure

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

Before you execute this command, make sure automated underlay network deployment is enabled.

Examples

Display information about automated underlay network deployment.

```
<Sysname> display vcf-fabric underlay autoconfigure
success command:
       #
         system
         clock timezone beijing add 08:00:00
       #
         system
         lldp global enable
       #
         system
         stp global enable
       #
         system
         interface Vlan-interface1
         ip address dhcp-alloc
       #
         system
         telnet server enable
       #
         system
         ssh server enable
       #
         system
         info-center loghost 110.0.0.111
       #
         system
         local-user aaa
```

```
 password ******
 service-type telnet http https ssh
 authorization-attribute user-role network-admin
#
 system
 line vty 0 63
 authentication-mode scheme
 user-role network-admin
#
 system
 vcf-fabric topology enable
#
 system
 snmp-agent
 snmp-agent community read public
 snmp-agent community write private
 snmp-agent sys-info version all
#
 system
 vlan 4093
#
 system
 vlan 4094
#
 system
 interface Vlan-interface4094
 ip address dhcp-alloc
#
 system
 ntp-service enable
 ntp-service unicast-server 110.0.0.111
#
 system
 snmp-agent
 snmp-agent community read public
 snmp-agent community write private
 snmp-agent sys-info version all
 snmp-agent packet max-size 4096
 snmp-agent target-host trap address udp-domain 110.0.0.111 params securityname
public v2c
#
 system
 telnet server enable
 local-user 2
 password ******
 service-type telnet http https
 authorization-attribute user-role network-admin
#
 system
```

```
  ssh server enable
  local-user 3
  password ******
  service-type ssh http https
  authorization-attribute user-role network-admin
 #
  system
  netconf soap http enable
  netconf soap https enable
  local-user 1
  password ******
  service-type http https
  authorization-attribute user-role network-admin
 #
IRF allocation:
       Self Bridge Mac: 00e0-fc00-510a
       IRF Status: No
       Member List: [1]
```

Table 2 Command output

Field	Description
success command	Commands that have been successfully executed during automated underlay network deployment.
Uplink interface	Uplink interfaces of the device.
Downlink interface	Downlink interfaces of the device.
Aggregation configuration	Information about Layer 2 aggregation groups.
IRF allocation	IRF configurations, including IRF bridge MAC address of the IRF fabric, IRF status, and the IRF member ID of the device.

Related commands

vcf-fabric underlay autoconfigure

display vcf-fabric underlay template-version

Use **display vcf-fabric underlay template-version** to display the supported version and the current version of the template file for automated VCF fabric deployment.

Syntax

display vcf-fabric underlay template-version

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

The version format of a template file for automated VCF fabric deployment is *x*.*y*. Only the *x* part is examined during a version compatibility check. For successful automated deployment, make sure *x* in the version of the template file to be used is not greater than *x* in the supported version.

Examples

Display the supported version and the current version of the template file for automated VCF fabric deployment when automated deployment is not started.

```
<Sysname> display vcf-fabric underlay template-version
Supported template version: 6.0
Current template version: Not available
```

Display the supported version and the current version of the template file for automated VCF fabric deployment when automated deployment has finished.

```
<Sysname> display vcf-fabric underlay template-version
Supported template version: 6.0
Current template version: 6.0
```

Table 3 Command output

Field	Description
Supported template version	Supported version of the template file for automated VCF fabric deployment.
Current template version	Current version of the template file for automated VCF fabric deployment. This field displays **Not available** if automated VCF fabric deployment has not started. This field displays **None** if automated VCF fabric deployment has finished but the template file does not contain a version number.

vcf-fabric topology enable

Use **`vcf-fabric topology enable`** to enable VCF fabric topology discovery.

Use **`undo vcf-fabric topology enable`** to disable VCF fabric topology discovery.

Syntax

`vcf-fabric topology enable`

`undo vcf-fabric topology enable`

Default

VCF fabric topology discovery is disabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable VCF fabric topology discovery.

```
<Sysname> system-view
[Sysname] vcf-fabric topology enable
```

vcf-fabric underlay autoconfigure

Use **vcf-fabric underlay autoconfigure** to specify the template file for automated underlay network deployment.

Use **undo vcf-fabric underlay autoconfigure** to restore the default.

Syntax

vcf-fabric underlay autoconfigure *template*

undo vcf-fabric underlay autoconfigure

Default

No template file is specified for automated underlay network deployment.

Views

System view

Predefined user roles

network-admin

Parameters

template: Specifies a template file by its name, a case-insensitive string of 1 to 127 characters. A template file is a file ending with the **.template** file extension.

Usage guidelines

After this command is executed, the device uses the specified template file to deploy the underlay network.

Examples

Specify template file **1_access.template** for automated underlay network deployment.

```
<Sysname> system-view
[Sysname] vcf-fabric underlay autoconfigure 1_access.template
```

vcf-fabric underlay pause

Use **vcf-fabric underlay pause** to pause automated underlay network deployment.

Use **undo vcf-fabric underlay pause** to continue automated underlay network deployment.

Syntax

vcf-fabric underlay pause

undo vcf-fabric underlay pause

Default

Automated underlay network deployment is not paused.

Views

System view

Predefined user roles

network-admin

Usage guidelines

You can use this command to pause automated underlay network deployment if the device is in the process of automated underlay network deployment.

Examples

Pause automated underlay network deployment.

```
<Sysname> system-view
[Sysname] vcf-fabric underlay pause
```

Contents

Cloud connection commands

The S3100V3-EI switch series does not support cloud connections.

cloud-management keepalive

Use **cloud-management keepalive** to set the keepalive interval for the local device to send keepalive packets to the H3C cloud server.

Use **undo cloud-management keepalive** to restore the default.

Syntax

cloud-management keepalive *interval*

undo cloud-management keepalive

Default

The keepalive interval is 180 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the keepalive interval in the range of 180 to 600 seconds.

Usage guidelines

If the device does not receive a response from the H3C cloud server within three keepalive intervals, the device sends a registration request to re-establish the cloud connection.

Examples

Set the keepalive interval to 360 seconds.

```
<Sysname> system-view
[Sysname] cloud-management keepalive 360
```

cloud-management server domain

Use **cloud-management server domain** to configure the domain name of the H3C cloud server.

Use **undo cloud-management server domain** to restore the default.

Syntax

cloud-management server domain *domain-name*

undo cloud-management server domain

Default

The default settings are as follows:

- The domain name of the cloud server is not configured for the S5130S-HI, S5130S-EI, S3100V3-EI, E500C, E500D, and E128C & E152C switch series.
- For the S5130S-SI and S5120V2-SI switch series:

- The domain name of the cloud server is not configured for a switch that starts up with the initial configuration.
- The domain name of the cloud server is **oasis.h3c.com** for a switch that starts up with the factory defaults.

For more information about the initial configuration and factory defaults, see *Fundamentals Configuration Guide*.

Views

System view

Predefined user roles

network-admin

Parameters

domain-name: Specifies the domain name of the H3C cloud server, a case-sensitive string of 1 to 253 characters.

Usage guidelines

Before you configure the domain name of the H3C cloud server, make sure a DNS server has been configured to translate the domain name.

If you execute the command multiple times, the most recent configuration takes effect.

Examples

Configure the domain name of the H3C cloud server as **abc.com**.

```
<Sysname> system-view
[Sysname] cloud-management server domain abc.com
```

cloud-management server password

Use **cloud-management server password** to set the password for establishing cloud connections to the cloud server.

Use **cloud-management server password** to restore the default.

NOTE:

This command is supported only in Release 6328 and later.

Syntax

cloud-management server password { **cipher** | **simple** } *string*

undo cloud-management server password

Default

No password is set for establishing cloud connections to the cloud server.

Views

System view

Predefined user roles

network-admin

mdc-admin

Parameters

cipher: Specifies the password in encrypted form.

simple: Specifies the password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. The plaintext form is a case-sensitive string of 1 to 63 characters. The encrypted form is a case-sensitive string of 1 to 117 characters.

Usage guidelines

After you change the password, the device terminates the cloud connections that have been established (if any) and uses the new password to establish cloud connections.

Examples

Set the password for establishing cloud connections to the cloud server to **12345678TESTplat&!** in plaintext format.

```
<Sysname> system-view
[Sysname] cloud-management server password simple 12345678TESTplat&!
```

display cloud-management state

Use **display cloud-management state** to display cloud connection state information.

Syntax

display cloud-management state

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display cloud connection state information.

```
<Sysname> display cloud-management state
Cloud connection state   : Established
Device state             : Request_success
Cloud server address     : 10.1.1.1
Cloud server domain name : abc.com
Cloud server port        : 443
Connected at             : Wed Jan  27 14:18:40 2016
Duration                 : 00d 00h 02m 01s
Process state            : Message received
Failure reason           : N/A
```

Table1-1 Command output

Field	Description
Cloud connection state	Cloud connection state: **Unconnected**, **Request**, and **Established**.
Device state	Local device state: • **Idle**—In idle state. • **Connecting**—Connecting to the H3C cloud server. • **Request_CAS_url**—Sent a central authentication service (CAS) URL

Field	Description
	request. • **Request_CAS_url_success**—Requesting CAS URL succeeded. • **Request_CAS_TGT**—Sent a ticket granting ticket (TGT) request. • **Request_CAS_TGT_success**—Requesting TGT succeeded. • **Request_CAS_ST**—Sent a service ticket (ST) request. • **Request_CAS_ST_success**—Requesting ST succeeded. • **Request_cloud_auth**—Sent an authentication request. • **Request_cloud_auth_success**—Authentication succeeded. • **Register**—Sent a registration request. • **Register_success**—Registration succeeded. • **Request**—Sent a handshake request. • **Request_success**—Handshake succeeded.
Cloud server address	IP address of the H3C cloud server.
Cloud server domain name	Domain name of the H3C cloud server.
Cloud server port	TCP port number used to establish cloud connections.
Connected at	Time when the cloud connection was established.
Duration	Duration since the establishment of the cloud connection.
Process state	Cloud connection processing state: • DNS not parsed. • DNS parsed. • Message not sent. • Message sent. • Message not received. • Message received.
Failure reason	Cloud connection failure reason: • DNS parse failed. • Socket connection failed. • SSL creation failed. • Sending CAS url request failed. • Sending CAS TGT failed. • Sending CAS ST failed. • Sending cloud auth request failed. • Sending registration request failed. • Processing CAS URL response failed. • Processing CAS TGT response failed. • Processing CAS ST response failed. • Processing cloud auth response failed. • Processing registration response failed. • Sending handshake request failed. • Processing handshake failed. • Sending websocket request failed. • Processing websocket packet failed.

reset cloud-management tunnel

Use **reset cloud-management tunnel** to re-establish the cloud connection to the H3C cloud server.

Syntax

reset cloud-management tunnel

Views

User view

Predefined user roles

network-admin

Examples

Re-establish the cloud connection to the H3C cloud server.

```
<Sysname> reset cloud-management tunnel
```

Contents

SmartMC commands

boot-loader file

Use **boot-loader file** to specify the upgrade startup software files for a SmartMC group.

Use **undo boot-loader** to restore the default.

Syntax

boot-loader file { *ipe-filename* | **boot** *boot-filename* **system** *system-filename* }

undo boot-loader

Default

No upgrade startup software files are specified for a SmartMC group.

Views

SmartMC group view

Predefined user roles

network-admin

Parameters

ipe-filename: Specifies an IPE software file by its name, a case-insensitive string of 5 to 45 characters. The file name must include the **.ipe** extension.

boot *boot-filename*: Specifies a boot image file by its name, a case-insensitive string of 5 to 45 characters. The file name must include the **.bin** extension.

system *system-filename*: Specifies a system image file by its name, a case-insensitive string of 5 to 45 characters. The file name must include the **.bin** extension.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify IPE software file **device.ipe** for SmartMC group **testgroup**.

```
<Sysname> system-view
[Sysname] smartmc group testgroup
[Sysname-smartmc-group-testgroup] boot-loader file device.ipe
```

Related commands

smartmc group

smartmc upgrade boot-loader

create batch-file

Use **create batch-file** to create a batch file.

Syntax

create batch-file *batch-file-name*

Default

No batch files exist.

Views

User view

Predefined user roles

network-admin

Parameters

batch-file-name: Specifies the name of the batch file, a case-insensitive string of 1 to 255 characters. If you do not specify a file extension when specifying a file name, the default extension **.cmdset** is used.

Usage guidelines

After executing this command, you will enter the batch edit mode. In this mode, each command occupies a line. When you finish editing all command lines, enter a percent sign (%) to return to user view.

Make sure the command lines that you enter are correct because the system does not verify whether the command lines are correct.

Examples

Create a batch file named **test.cmdset**, and enter the command lines for specifying the device name as **Sysname** and enabling Telnet.

```
<Sysname> create batch-file test.cmdset
Begin to edit batch commands, and quit with the character '%'.
system-view
sysname Sysname
telnet server enable%
<Sysname>
```

Related commands

display smartmc batch-file status

smartmc batch-file deploy

display smartmc backup configuration status

Use **display smartmc backup configuration status** to display the backup status on members.

Syntax

display smartmc backup configuration status

Views

Any view

Predefined user roles

network-admin

Usage guidelines

This command displays the status of the ongoing backup task or the most recent backup task if the member is not performing backup.

Examples

Display the backup status on members.

```
<Sysname> display smartmc backup configuration status
ID     IpAddress        MacAddress          Status       Time
1      192.168.56.30    08d2-38ff-0300      Finished     2017-04-05 11:30:35
2      192.168.56.40    62d2-c21c-0400      Finished     2017-04-05 11:30:40
```

Table 1 Command output

Field	Description
ID	ID of the member.
IpAddress	IP address of the member.
MacAddress	MAC address of the member.
Status	Backup status: • **Waiting**—The member is waiting for configuration backup. • **Processing**—The member is backing up the configuration. • **Finished**—The member has finished backing up the configuration. • **Timeout**—Configuration backup times out. • **Failed**—The member failed to back up the configuration.
Time	Time when the member finished backing up the configuration. If the member has not finished backing up the configuration, this field displays a hyphen (**-**).

Related commands

smartmc backup configuration

smartmc backup configuration interval

smartmc backup configuration max-number

display smartmc batch-file status

Use **display smartmc batch-file status** to display the batch file deployment result.

Syntax

display smartmc batch-file status [**ap** | **last** *number* | **phone**]

Views

Any view

Predefined user roles

network-admin

Parameters

ap: Displays the result of the most recent batch file deployment for ports connected to APs.

last *number*: Specifies a batch file deployment (performed by using the **smartmc batch-file deploy** command) by its number counting from the most recent batch file deployment. The value range for the *number* argument is 1 to 5.

phone: Displays the result of the most recent batch file deployment for ports connected to IP phones.

Usage guidelines

If you do not specify any parameters, this command displays the result of the most recent batch file deployment performed by using the **smartmc batch-file deploy** command.

Examples

Display the result of the most recent batch file deployment. In this example, the batch file contains the **display smartmc configuration** command.

```
<Sysname> display smartmc batch-file status last 1
TC ID 1
Device MAC : 8a73-60c3-0200
Start Time : 2018-12-24 14:55:39
End   Time : 2018-12-24 14:55:43
Result     :

<Sysname>display smartmc configuration
Device role              : TC
TM IP                    : 192.168.22.103
TM MAC                   : 8a73-4faa-0100
TM sysname               : Sysname
<Sysname>

TC ID 2
Device MAC : 8a73-6b31-0300
Start Time : 2018-12-24 14:55:43
End   Time : 2018-12-24 14:55:48
Result     :

<Sysname>display smartmc configuration
Device role              : TC
TM IP                    : 192.168.22.103
TM MAC                   : 8a73-4faa-0100
TM sysname               : Sysname
<Sysname>
```

Table 2 Command output

Field	Description
TC ID	ID of the member.
Device MAC	MAC address of the member.
Start Time	Batch file deployment start time.
End Time	Batch file deployment end time.
Result	Batch file deployment result in details.

Related commands

create batch-file

smartmc batch-file apply

smartmc batch-file deploy

display smartmc configuration

Use **display smartmc configuration** to display the SmartMC configuration.

Syntax

display smartmc configuration

Views

Any view

Predefined user roles

network-admin

Examples

Display the SmartMC configuration on the commander.

Release 6318P01 and earlier:

```
<Sysname> display smartmc configuration
Device role                          : TM
FTP server IP                        : 192.168.22.103
FTP server username                  : admin
Topology-refresh interval            : 60(s)
Backup startup-configuration interval : N/A
Sync backup number                   : 5
Device status                        : Lack
Some configurations are absent on the TM, such as Telnet or LLDP configuration.
```

Release 6328 and later:

```
<Sysname> display smartmc configuration
Device role                          : TM
File server:
  Type: FTP
  IP address: 192.168.22.103
  Username: admin
  Port: 21
  VPN instance: N/A
  Directory: /FTP
Topology-refresh interval            : 60(s)
Backup startup-configuration interval : N/A
Sync backup number                   : 5
Device status                        : Lack
Some configurations are absent on the TM, such as Telnet or LLDP configuration.
```

Display the commander information on a member.

```
<Sysname> display smartmc configuration
Device role       : TC
TM IP             : 192.168.22.103
TM MAC            : 8288-468d-0100
TM sysname        : Sysname
```

Table 3 Command output

Field	Description
Device role	Role of the device.
FTP server IP	This field is supported only in Release 6318P01 and earlier. IP address of the FTP server. If no FTP server IP address is configured, this field displays **N/A**.
FTP server username	This field is supported only in Release 6318P01 and earlier. FTP server username. If no username is configured, this field displays **N/A**.
File server	This field is supported only in Release 6328 and later. File server configuration.
Type	This field is supported only in Release 6328 and later. File server type. If no file server is specified, this field displays **N/A**.
IP address	This field is supported only in Release 6328 and later. File server IP address. If no file server is specified, this field displays **N/A**.
Username	This field is supported only in Release 6328 and later. File server username. If no file server is specified, this field displays **N/A**.
Port	This field is supported only in Release 6328 and later. File server port. If no file server is specified, this field displays **N/A**.
VPN instance	This field is supported only in Release 6328 and later. VPN instance to which the file server belongs. If no file server is specified, this field displays **N/A**.
Directory	This field is supported only in Release 6328 and later. Storage directory of files on the file server. If no file server is specified, this field displays **N/A**.
Topology-refresh interval	Topology refresh interval, in seconds.
Backup startup-configuration interval	Automatic configuration file backup interval, in hours. If no interval is set, this field displays **N/A**.
Sync backup number	Number of members that can perform configuration backup at the same time.
Device status	Commander status: • **Normal**. • **Lack**—Lack of configuration, such as NETCONF, Telnet, local user, and LLDP.
TM IP	IP address of the commander. If the member failed to obtain the commander IP address, this field displays **N/A**.
TM MAC	MAC address of the commander, If the member failed to obtain the commander MAC address, this field displays **N/A**.
TM sysname	Name of the commander. If the member failed to obtain the commander name, this field displays **N/A**.
Some configurations are absent on the TM, such as XXX.	This field is available only when the **Device status** field displays **Lack**. Lack of configuration will affect SmartMC functions. Please follow the prompt to complete the configuration.

Related commands

`smartmc backup configuration interval`

smartmc backup configuration max-number

smartmc enable

smartmc { **ftp-server** | **sftp-server** }

smartmc topology-refresh interval

display smartmc device-link

Use **display smartmc device-link** to display connections between devices in the SmartMC network.

Syntax

display smartmc device-link

Views

Any view

Predefined user roles

network-admin

Examples

Display connections between devices in the SmartMC network.

```
<Sysname> display smartmc device-link
(TM IP)[192.168.56.20]
ID    Hop  LocalPort            LocalIP           PeerPort              PeerIP
0     0    GigabitEthernet1/0/2  192.168.56.20    GigabitEthernet1/0/1  192.168.56.30
1     1    GigabitEthernet1/0/1  192.168.56.30    GigabitEthernet1/0/2  192.168.56.20
1     2    GigabitEthernet1/0/2  192.168.56.30    GigabitEthernet1/0/1  192.168.56.40
2     3    GigabitEthernet1/0/1  192.168.56.40    GigabitEthernet1/0/2  192.168.56.30
```

Table 4 Command output

Field	Description
TM IP	IP address of the commander.
ID	ID of the commander or member.
Hop	Number of hops between the commander and member.
LocalPort	Local port.
LocalIP	IP address of the local device.
PeerPort	Peer port.
PeerIP	IP address of the peer port.

Related commands

smartmc topology-refresh

smartmc topology-refresh interval

display smartmc group

Use **display smartmc group** to display SmartMC group information.

Syntax

display smartmc group [*group-name*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

Parameters

group-name: Specifies a SmartMC group by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this argument, the command displays information about all SmartMC groups.

Verbose: Displays detailed SmartMC group information. If you do not specify this keyword, the command displays brief SmartMC group information.

Examples

Display detailed SmartMC group information.

```
<Sysname> display smartmc group verbose
Group name                    : test
TC count                      : 3
Boot-loader file              :
Startup-configuration file    :
Rule:
 Match Device-type S5130S-LI
TCID DeviceType Sysname  IpAddress       MacAddress     Status   Version
1    S5130S-LI  S1       192.168.56.103  0e74-e2fb-0400 Normal   COMWAREV700R001
2    S5130S-LI  S2       192.168.56.102  0e74-ea13-0500 Normal   COMWAREV700R001
3    S5130S-LI  S3       192.168.56.104  0e74-db54-0300 Normal   COMWAREV700R001
```

Table 5 Command output

Field	Description
GroupName	Name of the SmartMC group.
TC count	Number of members in the SmartMC group.
Boot-loader file	Names of the upgrade startup software files for upgrading the SmartMC group. If no upgrade startup software files are specified, this field displays null.
Startup-configuration file	Name of the configuration file for upgrading the SmartMC group. If no configuration file is specified, this field displays null.
Rule	Match criteria of the SmartMC group.
Match	Match type and its value. The match types include the following: • **Device-type**—Matches members by device type. • **IP-address**—Matches members by IP address. • **MAC-address**—Matches members by MAC address.
TCID	ID of the member.
DeviceType	Device type of the member.
Sysname	Device name of the member.
IpAddress	IP address of the member.
MacAddress	MAC address of the member.

Field	Description
Version	Software version of the member.
Status	Operating status of the member: • **Offline**—The member is offline. • **Normal**—The member is online.

Related commands

match

smartmc group

display smartmc replace status

Use **display smartmc replace status** to display faulty member replacement status.

Syntax

display smartmc replace status

Views

Any view

Predefined user roles

network-admin

Examples

Display faulty member replacement status.

```
<Sysname> display smartmc replace status
Faulty ID      : 2
Faulty MAC     : 94e2-cdcb-0600
Replacement ID : 3
Replacement MAC: 2443-5f8c-0200
Mode           : Manual
Status         : Successful
Start time     : 2017-03-21 15:01:31
End time       : 2017-03-21 15:01:40
```

Table 6 Command output

Field	Description
Faulty ID	ID of the faulty member.
Faulty MAC	MAC address of the faulty member.
Replacement ID	ID of the new member.
Replacement MAC	MAC address of the new member.
Mode	Replacement method, which can be **Manual** or **Auto**.
Status	Replacement status: • **Successful**. • **Failed**. • **Replacing**. • **Timeout**.

Field	Description
Start time	Replacement start time
End time	Replacement end time.

Related commands

smartmc auto-replace enable

smartmc replace

display smartmc resource-monitor

Use **display smartmc resource-monitor** to display resource monitoring information.

Syntax

display smartmc resource-monitor [**cpu** | **memory** | **temperature**] * [**tc** *tc-id* | **tm**]

Views

Any view

Predefined user roles

network-admin

Parameters

cpu: Displays CPU usage.

memory: Displays memory usage.

temperature: Displays temperature information.

tc *tc-id*: Specify a member by its ID in the range of 1 to 255.

tm: Specify the commander.

Usage guidelines

This command displays CPU usage, memory usage, and temperature information of the commander and members on the commander. For packet dropping information, log in to the Web interface of the commander and access the **SmartMC** > **Intelligent O&M** > **Resource monitoring** page. Packet dropping information can be viewed only in Release 6328 and later.

If you do not specify a resource type, this command displays the resource monitoring information of all types.

If you do not specify a member or the commander, this command displays the resource monitoring information for the commander and all members.

Examples

Display the resource monitoring information for member 1.

```
<Sysname> display smartmc resource-monitor tc 1
TC 1
  Collection time : 2017-07-25 18:02:30
  Slot 1:
    CPU 0 CPU usage: 1%
    Memory usage   : 587076/903332
    Temperature    : 30
```

Table 7 Command output

Field	Description
Collection time	Time when the resource monitoring information was collected.

Related commands

smartmc resource-monitor

display smartmc resource-monitor configuration

Use **display smartmc resource-monitor configuration** to display resource monitoring configuration.

Syntax

display smartmc resource-monitor configuration

Views

Any view

Predefined user roles

network-admin

Usage guidelines

This command displays CPU usage, memory usage, and temperature monitoring configuration of the commander. In Release 6328 and later, you can view the status of packet dropping monitoring by using the **display current-configuration | include smartmc** command.

Examples

Display resource monitoring configuration.

```
<Sysname> display smartmc resource-monitor configuration
ID  MacAddress      CPU  Memory  Temperature
1   1111-2222-3333  Y    N       N
2   1111-2222-3334  Y    N       N
3   1111-2222-3335  Y    N       N
```

Table 8 Command output

Field	Description
ID	Device ID.
MacAddress	MAC address of the device.
CPU	CPU usage monitoring status: • **Y**—CPU usage monitoring is enabled. • **N**—CPU usage monitoring is disabled. • **-**—The device does not support CPU usage monitoring.
Memory	Memory usage monitoring status: • **Y**—Memory usage monitoring is enabled. • **N**—Memory usage monitoring is disabled. • **-**—The device does not support memory usage monitoring.
Temperature	Temperature monitoring status: • **Y**—Temperature monitoring is enabled. • **N**—Temperature monitoring is disabled.

Field	Description
	• -—The device does not support temperature monitoring.

Related commands

smartmc resource-monitor

display smartmc tc

Use **display smartmc tc** to display member information.

Syntax

display smartmc tc [*tc-id*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

Parameters

tc-id: Specifies a member by its ID in the range of 1 to 255. If you do not specify a member, this command displays information about all members.

verbose: Displays detailed member information. If you do not specify this keyword, the command displays brief member information.

Examples

Display brief information about all members.

```
<Sysname> display smartmc tc
TCID DeviceType Sysname  IpAddress       MacAddress     Status   Version
1    S5130S-LI  S1       192.168.22.104  201c-e7c3-0300 Normal   COMWAREV700R001
```

Table 9 Command output

Field	Description
TCID	ID of the member.
DeviceType	Device type of the member.
Sysname	Device name of the member.
IpAddress	IP address of the member.
MacAddress	MAC address of the member.
Status	Operating status of the member: • **Normal**—The member is operating correctly. • **Offline**—The member is offline.
Version	Software version of the member.

Display detailed information about all members.

```
<Sysname> display smartmc tc verbose
TC ID                       : 1
Adding method               : Manual
Sysname                     : S1
```

```
Model                          : S5130S-LI
Device type                    : S5130S-LI
SYSOID                         : 1.3.6.1.4.1.25506
MAC address                    : 0e74-e2fb-0400
IP address                     : 192.168.56.103
Boot image                     :
Boot image version             :
System image                   :
System image version           :
Current-configuration file     :
Uptime                         : 2 days, 3 hours, 4 minutes
System CPU usage               : 0%
System memory usage            : 0%
Status                         : Offline
Boot-loader file               :
Startup-configuration file     :
```

Table 10 Command output

Field	Description
TC ID	ID of the member.
Adding method	Method through which the member is added to the SmartMC network: • Manual. • Auto.
Sysname	Device name of the member.
Model	Device model of the member.
Device type	Device type of the member.
SYSOID	SYSOID of the member.
MAC address	MAC address of the member.
IP address	IP address of the member.
Boot image	Boot image file that the member runs.
Boot image version	Version of the boot image file.
System image	System image file that the member runs.
System image version	Version of the system image file.
Current-configuration file	Current startup configuration file used by the member.
Uptime	Operation duration of the member.
System CPU usage	CPU usage on the member.
System memory usage	Memory usage on the member.
Status	Operating status of the member: • **Normal**—The member is operating correctly. • **Offline**—The member is offline.
Boot-loader file	Upgrade startup software files.
Startup-configuration file	Upgrade configuration file.

display smartmc tc log buffer

Use **display smartmc tc log buffer** to display log information in the log buffer on a member.

Syntax

display smartmc tc *tc-id* **log buffer** [**module** *module-name* [**mnemonic** *mnemonic-value*]]

Views

Any view

Predefined user roles

network-admin

Parameters

tc-id: Specifies a member by its ID in the range of 1 to 255.

module *module-name*: Specifies a module by its name, a case-insensitive string of 1 to 8 characters. To display module names, use the **info-center source** command (see information center commands in *Network Management and Monitoring Command Reference*).

mnemonic *mnemonic-value*: Specifies a mnemonic, a case-insensitive string of 1 to 32 characters.

Examples

Display the log information for the SHELL module with the SHELL_CMD mnemonic for member 1.

```
<Sysname> display smartmc tc 1 log buffer module SHELL mnemonic SHELL_CMD
Time     : 2017-07-15 13:51:46
Level    : Informational
Module   : SHELL
Mnemonic : SHELL_CMD
Content  : -Line=con0-IPAddr=**-User=**; Command is qu

Time     : 2017-07-15 13:51:39
Level    : Informational
Module   : SHELL
Mnemonic : SHELL_CMD
Content  : -Line=con0-IPAddr=**-User=**; Command is local-user admin
```

Table 11 Command output

Field	Description
Time	Time when the log was generated.
Level	Log level.

display smartmc tc log restart

Use **display smartmc tc log restart** to display the restart log information for a member.

Syntax

display smartmc tc *tc-id* **log restart**

Views

Any view

Predefined user roles

network-admin

Parameters

tc-id: Specifies a member by its ID in the range of 1 to 255.

Usage guidelines

In addition to saving the logs generated by modules to the log buffer, a member sends restart logs to the commander. The commander creates a restart log buffer for each member to store their restart logs.

The commander stores a maximum of 10 restart logs for each member. The most recent restart log overwrites the oldest one when there are more than 10 restart logs for a member.

You can also use the **display smartmc tc** *tc-id* **log buffer module** SYSLOG **mnemonic** SYSLOG_RESTART command to display the restart log information.

Examples

Display the restart log information for member 1.

```
<Sysname> display smartmc tc 1 log restart
Time     : 2017-07-15 13:51:46
Level    : Informational
Module   : SYSLOG
Mnemonic : SYSLOG_RESTART
Content  : System restarted -- H3C Comware Software.
```

Table 12 Command output

Field	Description
Time	Time when the log was generated.
Level	Log level.

Related commands

display smartmc tc log buffer

display smartmc upgrade status

Use **display smartmc upgrade status** to display member upgrade status.

Syntax

display smartmc upgrade status

Views

Any view

Predefined user roles

network-admin

Examples

Display member upgrade status.

```
<Sysname> display smartmc upgrade status
```

```
ID    IpAddress         MacAddress      Status      UpdateTime        UpdateFile
1     192.168.56.1      82dd-a434-0200  Finished    Immediately       bootloader.ipe
2     192.168.56.103    5caf-2e5f-0100  Finished    Immediately       bootloader.ipe
```

Table 13 Command output

Field	Description
ID	ID of the member.
MacAddress	MAC address of the member.
IpAddress	IP address of the member.
Status	Upgrade status: • **Waiting**—The member is waiting for downloading the upgrade file. • **Download-failed**—The member failed to download the upgrade file. • **Download-finished**—The member has downloaded the upgrade file. • **Downloading**—The member is downloading the upgrade file. • **Updating**—The member is upgrading. • **Finished**—The member has finished upgrading. • **Failed**—The member failed to upgrade. • **Unknown**—The upgrade status of the member is unknown.
Updated File	Name of the upgrade file.
UpdateTime	Upgrade time: • **Immediately**—Upgrade at once. • **Delay(m)**—Upgrade after the specified delay. • **Time(HH:MM)**—Upgrade at the specified time.

Related commands

`smartmc upgrade group`

`smartmc upgrade tc`

display smartmc vlan

Use **`display smartmc vlan`** to display VLAN creation results for members.

Syntax

`display smartmc vlan`

Views

Any view

Predefined user roles

network-admin

Examples

Display VLAN creation results.

```
<Sysname> display smartmc vlan
ID     IpAddress         MacAddress        Vlan      Status
1      192.168.22.222    703d-15ad-cd02    2         Success
2      192.168.22.3      24ff-2264-0100    2         Success
3      192.168.22.4      24ff-2f74-0200    2         Success
4      192.168.22.223    487a-dac8-29ba    2         Success
```

Table 14 Command output

Field	Description
ID	Member ID.
IpAddress	IP address of the member.
MacAddress	MAC address of the member.
Vlan	VLAN created for the member.
Status	VLAN creation status: • **Processing**—The VLAN is being created. • **Success**—The VLAN has been created successfully. • **Failure. The port xxx is not an access port**—The VLAN fails to be created, because ports connected to non-SmartMC devices are not access ports. • **Failure. xxx not exist**—The VLAN fails to be created, because all access ports are connected to SmartMC devices.

Related commands

smartmc vlan

match

Use **match** to set a match criterion to add all matching members to a SmartMC group.

Use **undo match** to delete a match criterion.

Syntax

match { **device-type** *device-type* | **ip-address** *ip-address* { *ip-mask-length* | *ip-mask* } | **mac-address** *mac-address mac-mask-length* }

undo match { **device-type** *device-type* | **ip-address** *ip-address* { *ip-mask-length* | *ip-mask* } | **mac-address** *mac-address mac-mask-length* }

Default

No match criterion is set.

Views

SmartMC group view

Predefined user roles

network-admin

Parameters

device-type *device-type*: Sets a device type match criterion.

ip-address *ip-address* { *ip-mask-length* | *ip-mask* }: Sets an IP address match criterion. The *ip-address* argument specifies an IP address in dotted decimal notation. The *ip-mask* argument specifies the subnet mask in dotted decimal notation. The *ip-mask-length* argument specifies the subnet mask length in the range of 1 to 32.

mac-address *mac-address mac-mask-length*: Sets a MAC address match criterion. The *mac-address* argument specifies a MAC address in the format of *H-H-H*. The *mac-mask-length* argument specifies the mask length in the range of 1 to 48.

Examples

Create a SmartMC group named **a** and add members in subnet 192.168.1.0/24 to the group.

```
<Sysname> system-view
[Sysname] smartmc group a
[Sysname-smartmc-group-a] match ip-address 192.168.1.0 24
```

Related commands

smartmc group

display smartmc group

smartmc auto-link-aggregation enable

Use **smartmc auto-link-aggregation enable** to enable automatic Ethernet link aggregation.

Use **undo smartmc auto-link-aggregation enable** to disable automatic Ethernet link aggregation.

Syntax

smartmc auto-link-aggregation enable

undo smartmc auto-link-aggregation enable

Default

Automatic Ethernet link aggregation is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Automatic Ethernet link aggregation is performed only between member devices.

Enabling or disabling automatic Ethernet link aggregation might cause network flapping, and the members might go offline for a short period of time.

Examples

Enable automatic Ethernet link aggregation.

```
<Sysname> system-view
[Sysname] smartmc auto-link-aggregation enable
```

smartmc auto-replace enable

Use **smartmc auto-replace enable** to enable the automatic faulty member replacement feature.

Use **undo smartmc auto-replace enable** to disable the automatic faulty member replacement feature.

Syntax

smartmc auto-replace enable

undo smartmc auto-replace enable

Default

The automatic faulty member replacement feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

To perform an automatic fault replacement, first enable this feature on the commander, and then perform the following tasks:

1. Install the new member at the location where the faulty member was installed.
2. Connect all cables to the new member.

Make sure the new member and the faulty member have the same neighbor relationship, device model, and IRF member ID.

Examples

Enable the automatic faulty member replacement feature.

```
<Sysname> system-view
[Sysname] smartmc auto-replace enable
```

Related commands

smartmc replace

smartmc backup configuration

Use **smartmc backup configuration** to manually back up the configuration file on members.

Syntax

smartmc backup configuration { **group** *group-name-list* | **tc** [*tc-id-list*] }

Views

System view

Predefined user roles

network-admin

Parameters

group *group-name-list*: Specifies a space-separated list of up to 10 SmartMC groups. The group name is a case-sensitive string of 1 to 31 characters.

tc *tc-id-list*: Specifies a space-separated list of up to 10 member items. Each item specifies a device or a range of devices in the form of *tc-id1* **to** *tc-id2*. The value for *tc-id2* must be greater than or equal to the value for *tc-id1*. The value range for the *tc-id* argument is 0 to 255, with 0 representing the commander and 1 to 255 representing members. If you do not specify the commander or any members, all devices will perform configuration backup.

Usage guidelines

After you execute this command, the members immediately save the running configuration to the next-startup configuration files and upload the configuration files to the file server.

The backup configuration files are named in the format of *bridge MAC address*_**backup.cfg**.

Examples

Back up the configuration file on member 1, member 2, member 3, and member 4.

```
<Sysname> system-view
[Sysname] smartmc backup configuration tc 1 to 4
```

Back up the configuration file on all members in SmartMC groups **test1**, **test2**, and **test3**.

```
<Sysname> system-view
[Sysname] smartmc backup configuration group test1 test2 test3
```

Related commands

display smartmc configuration

smartmc backup configuration interval

smartmc backup configuration max-number

Use **smartmc backup configuration max-number** to set the maximum number of members that can perform automatic configuration backup at the same time.

Use **undo smartmc backup configuration max-number** to restore the default.

Syntax

smartmc backup configuration max-number *max-number*

undo smartmc backup configuration max-number

Default

A maximum of five members can perform automatic configuration backup at the same time.

Views

System view

Predefined user roles

network-admin

Parameters

max-number: Specifies the maximum number of members that can perform automatic configuration backup at the same time, in the range of 2 to 20.

Usage guidelines

The maximum number of members that can perform automatic configuration at the same time is limited by the performance of the file server. If automatic configuration backup fails, set the maximum number of members to a smaller value.

Examples

Specify that a maximum of 10 members can perform automatic configuration backup at the same time.

```
<Sysname> system-view
[Sysname] smartmc backup configuration max-number 10
```

Related commands

display smartmc configuration

smartmc backup configuration

smartmc backup configuration interval

smartmc backup configuration interval

Use **smartmc backup configuration interval** to enable the automatic configuration file backup feature and set the automatic backup interval.

Use **undo smartmc backup configuration interval** to restore the default.

Syntax

smartmc backup configuration interval *interval*

undo smartmc backup configuration interval

Default

The automatic configuration file backup feature is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the automatic configuration file backup interval in the range of 1 to 720 hours.

Usage guidelines

This command enables the commander and members to back up their configuration files by saving the running configuration to the files and then uploading them to the file server. When you execute this command, the commander and members immediately perform a backup. After that, they back up the configuration files at the specified interval. The backup configuration files are named in the format of *bridge MAC address*_**backup.cfg**.

Examples

Enable the automatic configuration file backup feature and set the backup interval to 24 hours.

```
<Sysname> system-view
[Sysname] smartmc backup configuration interval 24
```

Related commands

display smartmc configuration

smartmc backup configuration

smartmc batch-file apply

Use **smartmc batch-file apply** to specify a batch file to deploy to ports connecting APs or IP phones.

Use **undo smartmc batch-file apply** to remove a batch file specified for ports connecting APs or IP phones.

Syntax

smartmc batch-file *batch-file-name* **apply** { **ap** | **phone** }

undo smartmc batch-file apply { **ap** | **phone** }

Default

No batch file is specified for ports connecting APs or IP phones.

Views

System view

Predefined user roles

network-admin

Parameters

batch-file-name: Specifies a batch file by its name, a case-insensitive string of 1 to 255 characters.

ap: Specifies ports connecting APs.

phone: Specifies ports connecting IP phones.

Usage guidelines

With batch file deployment enabled, the commander automatically deploys configurations in the specified batch file to a port connecting an AP or IP phone, simplifying access port configuration.

When the commander first detects the association of an AP or IP phone on a port through LLDP, it deploys the command lines in the specified batch file to the port. If no batch file is specified for the device type, the configurations on the port remain unchanged.

If the AP or IP phone disconnects from the port, the configurations on the port remain. When a new device comes online from the port, configurations used by the port depend on the new device type.

- If the new device is an AP or IP phone and has the same type as the disconnected device, the configurations on the port remain unchanged.
- If the new device is an AP or IP phone but has a different type as the disconnected device, the commander deploys the command lines in the specified batch file to the port. If no batch file is specified for the device type, the configurations on the port remain unchanged.
- If the new device is neither an AP nor an IP phone, the configurations on the port remain unchanged.

To disable the commander from deploying a batch file to ports, remove the specified batch file or execute the **undo smartmc batch-file-apply enable** command to disable batch file deployment. The **undo smartmc batch-file-apply enable** command is supported only in Release 6328 and later.

Examples

Specify batch file **ap.cmdset** for ports connecting APs or IP phones.

```
<Sysname> system-view
[Sysname] smartmc batch-file ap.cmdset apply ap
```

Related commands

create batch-file

smartmc batch-file-apply enable

smartmc batch-file deploy

Use **smartmc batch-file deploy** to deploy bulk command lines to a list of members or SmartMC groups.

Syntax

smartmc batch-file *batch-file-name* **deploy** { **group** *group-name-list* | **tc tc**-*id-list* }

Views

System view

Predefined user roles

network-admin

Parameters

batch-file-name: Specifies the name of a batch file, a case-insensitive string of 1 to 255 characters.

group *group-name-list*: Specifies a space-separated list of up to 10 SmartMC groups. The group name is a case-sensitive string of 1 to 31 characters.

tc *tc-id-list*: Specifies a space-separated list of up to 10 member items. Each item specifies a member or a range of members in the form of *tc-id1* **to** *tc-id2*. The value for *tc-id2* must be greater than or equal to the value for *tc-id1*. The value range for the *tc-id* argument is 1 to 255.

Examples

Deploy batch file **startup.cmdset** to SmartMC group **testgroup**.

```
<Sysname> system-view
[Sysname] smartmc batch-file startup.cmdset deploy group testgroup
```

Related commands

create batch-file

display smartmc batch-file status

smartmc batch-file-apply enable

Use **smartmc batch-file-apply enable** to enable batch file deployment.

Use **undo smartmc batch-file-apply enable** to disable batch file deployment.

NOTE:

This command is supported only in Release 6328 and later.

Syntax

smartmc batch-file-apply enable

undo smartmc batch-file-apply enable

Default

Batch file deployment is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

With batch file deployment enabled, the commander automatically deploys configurations in the specified batch file to a port connecting an AP or IP phone, simplifying access port configuration. To disable the commander from deploying a batch file to ports, remove the specified batch file or disable batch file deployment.

Examples

Disable batch file deployment.

```
<Sysname> system-view
[Sysname] undo smartmc batch-file-apply enable
```

Related commands

smartmc batch-file apply

smartmc enable

Use **smartmc enable** to enable SmartMC and set the device role.

Use **undo smartmc enable** to disable SmartMC.

Syntax

smartmc { **tc** | **tm** **username** *username* **password** { **cipher** | **simple** } *string* } **enable**

undo smartmc enable

Default

SmartMC is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

tc: Enables SmartMC and sets the device role to member.

tm: Enables SmartMC and sets the device role to commander.

username *username*: Specifies a username for the local user, a case-sensitive string of 1 to 55 characters.

password: Specifies a password for the local user.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 63 characters. Its encrypted form is a case-sensitive string of 1 to 117 characters.

Usage guidelines

A SmartMC network must have one and only one commander.

To enable SmartMC, execute this command on both the commander and members. To configure the other SmartMC features, execute associated commands only on the commander.

If you change the role of the commander to member or disable SmartMC on the commander, all SmartMC settings in its running configuration will be cleared.

SmartMC fails to be enabled if ACL resources are insufficient. If ACL resources are insufficient, use the **undo acl** command to delete unnecessary ACLs and then enable SmartMC. You can execute the **display acl** command to view ACL configuration and match statistics. For more information about ACLs, see *ACL and QoS Configuration Guide*.

SmartMC fails to be enabled if ports 80 and 443 have been used.

If you execute this command multiple times, the most recent configuration takes effect. You can execute the command to change the device role or the password.

Examples

Enable SmartMC and set the device role to member.

```
<Sysname> system-view
[Sysname] smartmc tc enable
```

smartmc { ftp-server | sftp-server }

Use **smartmc { ftp-server | sftp-server }** to configure the file server information.

Use **undo smartmc { ftp-server | sftp-server }** to delete the file server information.

Syntax

Release 6318P01 and earlier:

smartmc ftp-server *server-address* **username** *username* **password { cipher | simple }** *string*

undo smartmc ftp-server

Release 6328 and later:

smartmc { ftp-server | sftp-server } { *ipv4-address* | **ipv6** *ipv6-address* } [**port** *port*] [**vpn-instance** *vpn-instance-name*] [**directory** *directory*] **username** *username* **password { cipher | simple }** *string*

undo smartmc { ftp-server | sftp-server }

Default

No file server information is configured.

Views

System view

Predefined user roles

network-admin

Parameters

ftp-server: Specifies an FTP server.

sftp-server: Specifies an SFTP server.

ipv4-address: Specifies the IPv4 address of the file server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the file server.

port *port*: Specifies the port number of the file server, in the range of 1 to 65535. The default pot for an FTP server and an SFTP server is 21 and 22, respectively.

vpn-instance *vpn-instance-name*: Specifies the name of the MPLS L3VPN instance to which the file server belongs, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command considers that the file server is in the public network.

directory *directory*: Specifies the working directory of the file server, a case-insensitive string. By default, the root directory is used.

username *username*: Specifies the file server username, a case-sensitive string of 1 to 55 characters.

password: Specifies the file server password.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 63 characters. Its encrypted form is a case-sensitive string of 1 to 117 characters.

Usage guidelines

You can specify only one file server. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the file server type to FTP, and specify the server IP address, username, and password as 192.168.22.19, **admin**, and **hello12345**, respectively.

```
<Sysname> system-view
[Sysname] smartmc ftp-server 192.168.22.19 username admin password simple hello12345
```

Related commands

display smartmc configuration

smartmc group

Use **smartmc group** to create a SmartMC group and enter its view, or enter the view of an existing SmartMC group.

Use **undo smartmc group** to delete a SmartMC group.

Syntax

smartmc group *group-name*

undo smartmc group *group-name*

Default

No SmartMC groups exist.

Views

System view

Predefined user roles

network-admin

Parameters

group-name: Specifies the name of the SmartMC group, a case-sensitive string of 1 to 31 characters.

Usage guidelines

When you perform the following operations, you can specify a SmartMC group to apply the operations to all members in the group:

- Startup software upgrade.
- Configuration file upgrade.
- Configuration deployment.

Examples

Create SmartMC group **testgroup**.

```
<Sysname> system-view
[Sysname] smartmc group testgroup
[Sysname-smartmc-group-testgroup]
```

Related commands

match

smartmc outbound

Use **smartmc outbound** to configure an outgoing interface for the SmartMC network.

Use **undo smartmc outbound** to restore the default.

Syntax

smartmc outbound

undo smartmc outbound

Default

No interface is used as an outgoing interface, and the SmartMC network cannot communicate with outside networks.

Views

VLAN interface view

Predefined user roles

network-admin

Usage guidelines

VLAN interface 1 cannot be used as an outgoing interface, because the SmartMC network is established in VLAN 1.

Examples

Configure GigabitEthernet 1/0/1 as an outgoing interface for the SmartMC network.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] smartmc outbound
```

smartmc resource-monitor

Use **smartmc resource-monitor** to enable resource monitoring.

Use **undo smartmc resource-monitor** to disable resource monitoring.

Syntax

smartmc resource-monitor [**cpu** | **memory** | **packet-drop** | **temperature**] * [**group** *group-name-list* | **tc** { *tc-id-list* | **mac-address** *mac-address* } | **tm**]

undo smartmc resource-monitor [**cpu** | **memory** | **packet-drop** | **temperature**] * [**group** *group-name-list* | **tc** { *tc-id-list* | **mac-address** *mac-address* } | **tm**]

Default

Resource monitoring is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

cpu: Enables CPU usage monitoring.

memory: Enables memory usage monitoring.

packet-drop: Enables packet dropping monitoring.

NOTE:

The **packet-drop** keyword is supported only in Release 6328 and later.

temperature: Enables temperature monitoring.

group *group-name-list*: Specifies the SmartMC groups to monitor. You can specify a space-separated list of up to 10 SmartMC groups. The group name is a case-sensitive string of 1 to 31 characters.

tc: Specifies the members to monitor.

tc-id-list: Specifies a space-separated list of up to 10 member items. Each item specifies a member or a range of members in the form of *tc-id1* **to** *tc-id2*. The value for *tc-id2* must be greater than or equal to the value for *tc-id1*. The value range for the *tc-id* argument is 1 to 255.

mac-address *mac-address*: Specifies a member by its MAC address in the format of H-H-H.

tm: Enables resource monitoring on the commander.

Usage guidelines

Packet dropping monitoring monitors packet dropping on members and on interfaces.

If you do not specify a resource type, this command enables resource monitoring for all resource types.

If you do not specify a device to monitor (member or the commander), this command enables resource monitoring on the commander and all members.

Examples

Enable resource monitoring for all resource types on member 1 through member 3.

```
<Sysname> system-view
[Sysname] smartmc resource-monitor tc 1 to 3
```

Related commands

display smartmc resource-monitor

smartmc resource-monitor interval

smartmc resource-monitor max-age

smartmc resource-monitor interval

Use **smartmc resource-monitor interval** to set the interval for the commander to obtain resource monitoring information.

Use **undo smartmc resource-monitor interval** to restore the default.

Syntax

smartmc resource-monitor interval *interval*

undo smartmc resource-monitor interval

Default

The interval for the commander to obtain resource monitoring information is 1 minute.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the interval for the commander to obtain resource monitoring information, in the range of 1 to 60 minutes.

Usage guidelines

For packet dropping monitoring, the specified interval applies only to obtaining of member packet dropping information. Because of the great amount of interface information, the commander obtains interface packet dropping information from members only when Web displaying is requested.

Examples

Set the interval for the commander to obtain resource monitoring information to 5 minutes.

```
<Sysname> system-view
[Sysname] smartmc resource-monitor interval 5
```

Related commands

display smartmc resource-monitor

smartmc resource-monitor

smartmc resource-monitor max-age

Use **smartmc resource-monitor max-age** to set the aging time for resource monitoring information.

Use **undo smartmc resource-monitor max-age** to restore the default.

Syntax

smartmc resource-monitor max-age *max-age*

undo smartmc resource-monitor max-age

Default

The aging time for resource monitoring information is 24 hours.

Views

System view

Predefined user roles

network-admin

Parameters

max-age: Specifies the aging time for resource monitoring information, in the range of 1 to 168 hours.

Usage guidelines

For packet dropping monitoring, the specified aging time applies only to member packet dropping information. Each member saves its interface packet dropping information for as long as 30 days.

To view interface packet dropping information, log in to the Web interface of the commander and access the **SmartMC** > **Intelligent O&M** > **Resource monitoring** page. You can view information in the past 1 hour, 1 day, or 30 days.

Examples

Set the aging time for resource monitoring information to 1 hour.

```
<Sysname> system-view
[Sysname] smartmc resource-monitor max-age 1
```

Related commands

display smartmc resource-monitor

smartmc resource-monitor

smartmc replace

Use **smartmc replace** to manually replace a faulty member.

Syntax

smartmc replace tc *tc-id1* **faulty-tc** *tc-id2*

Views

System view

Predefined user roles

network-admin

Parameters

tc *tc-id1*: Specifies the ID of the new member, in the range of 1 to 255.

faulty-tc *tc-id2*: Specifies the ID of the faulty member, in the range of 1 to 255.

Usage guidelines

Before you execute this command, perform the following tasks:

1. Install the new member at the location where the faulty member was installed.
2. Connect all cables to the new member.

Make sure the new member and the faulty member have the same neighbor relationship, device model, and IRF member ID.

Examples

Replace faulty member 5 with new member 10.

```
<Sysname> system-view
[Sysname] smartmc replace tc 10 faulty-tc 5
```

Related commands

display smartmc replace status

smartmc auto-replace enable

smartmc tc boot-loader

Use **smartmc tc boot-loader** to specify the upgrade startup software files for a member.

Use **undo smartmc tc boot-loader** to remove the configuration.

Syntax

smartmc tc *tc-id* **boot-loader** { *ipe-filename* | **boot** *boot-filename* **system** *system-filename* }

undo smartmc tc *tc-id* **boot-loader**

Views

System view

Predefined user roles

network-admin

Parameters

tc *tc-id*: Specifies a member by its ID in the range of 1 to 255.

ipe-filename: Specifies an IPE software file by its name, a case-insensitive string of 5 to 45 characters. The file name must include the **.ipe** extension.

boot *boot-filename*: Specifies a boot image file by its name, a case-insensitive string of 5 to 45 characters. The file name must include the **.bin** extension.

system *system-filename*: Specifies a system image file by its name, a case-insensitive string of 5 to 45 characters. The file name must include the **.bin** extension.

Examples

Specify upgrade boot image **boot.bin** and upgrade system image **system.bin** for member 1.

```
<Sysname> system-view
[Sysname] smartmc tc 1 boot-loader boot boot.bin system system.bin
```

Related commands

display smartmc tc

smartmc tc device-type

Use **smartmc tc device-type** to define a member type on the commander.

Use **undo smartmc tc device-type** to delete a member type.

Syntax

smartmc tc sysoid *sysoid* **device-type** *device-type*

undo smartmc tc sysoid *sysoid* **device-type** *device-type*

Views

System view

Predefined user roles

network-admin

Parameters

sysoid *sysoid*: Specifies the SYSOID of a member.

device-type *device-type*: Specifies a member type.

Usage guidelines

A device type can correspond to multiple device models. You can identify different device models with different SYSOIDs by specifying a SYSOID for each device model. The commander identifies member types by SYSOID.

The system predefines the device types for some device models based on SYSOIDs. For device models without predefined device types, you must define their member types by SYSOID manually. If you do not do so, the commander cannot identify the types of such devices.

You cannot modify the predefined device types.

Before defining a device type for a member, you can use the **display smartmc tc** command to determine whether the member has a predefined one.

- If the member has been predefined with one device type, the **DeviceType** field displays the actual predefined device type.
- If the member does not have a predefined device type, the **DeviceType** field displays **unknown**.

To obtain the SYSOID of a member, use the **display smartmc tc verbose** command.

Examples

Define a member type by specifying the SYSOID as 1.3.6.1.4.1.25506.1.1588 and the member type as SW.

```
<Sysname> system-view
[Sysname] smartmc tc sysoid 1.3.6.1.4.1.25506.1.1588 device-type SW
```

smartmc tc password

Use **smartmc tc password** to modify the password for the default user (admin) on members.

Use **undo smartmc tc password** to restore the default.

Syntax

smartmc tc password [**cipher**] *string*

undo smartmc tc password

Default

The password for the default user on members is **admin**.

Views

System view

Predefined user roles

network-admin

Parameters

cipher: Specifies a password in encrypted form. If you do not specify this keyword, the command creates a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

NOTE:

The **cipher** keyword is supported only in Release 6328 and later.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 63 characters. Its encrypted form is a case-sensitive string of 33 to 117 characters.

Usage guidelines

During SmartMC network establishment, the commander establishes NETCONF sessions to members and adds them to the network. The default username and password on the members for NETCONF session establishment are **admin** and **admin**. To enhance security, you can perform this task to change the password for the default user **admin** of the members after the commander adds the members to the network.

If the default password cannot meet the password complexity requirements on members, you cannot execute the **undo smartmc tc password** command to restore the default.

Do not modify the password for members that are manually added to the SmartMC network. If you modify the password for a manually added member, you will not be able to manage that member from the commander.

Examples

Configure default user admin on members to use plaintext password **hello12345**.

```
<Sysname> system-view
[Sysname] smartmc tc password hello12345
```

smartmc tc startup-configuration

Use **smartmc tc startup-configuration** to specify the upgrade configuration file for a member.

Use **undo smartmc tc startup-configuration** to remove the configuration.

Syntax

smartmc tc *tc-id* **startup-configuration** *cfg-filename*

undo smartmc tc *tc-id* **startup-configuration**

Views

System view

Predefined user roles

network-admin

Parameters

tc *tc-id*: Specifies a member by its ID in the range of 1 to 255.

cfg-filename: Specifies a configuration file by its name, a case-insensitive string of 5 to 45 characters. The file name must include the **.cfg** extension.

Examples

Specify upgrade configuration file **startup.cfg** for member 1.

```
<Sysname> system-view
[Sysname] smartmc tc 1 startup-configuration startup.cfg
```

Related commands

display smartmc tc

smartmc topology-refresh

Use **smartmc topology-refresh** to manually refresh the network topology.

Syntax

smartmc topology-refresh

Views

Any view

Predefined user roles

network-admin

Usage guidelines

To display topology changes, use this command to manually refresh the topology.

Examples

Manually refresh the network topology.

```
<Sysname> smartmc topology-refresh
```

Related commands

display smartmc device-link

smartmc topology-refresh interval

Use **smartmc topology-refresh interval** to set the automatic network topology refresh interval.

Use **undo smartmc topology-refresh interval** to restore the default.

Syntax

smartmc topology-refresh interval *interval*

undo smartmc topology-refresh interval

Default

The automatic network topology refresh interval is 60 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the automatic network topology refresh interval in the range of 60 to 300 seconds.

Examples

Set the automatic network topology refresh interval to 100 seconds.

```
<Sysname> system-view
[Sysname] smartmc topology-refresh interval 100
```

Related commands

display smartmc device-link

smartmc topology-save

Use **smartmc topology-save** to save the current network topology.

Syntax

smartmc topology-save

Views

System view

Predefined user roles

network-admin

Usage guidelines

This task allows you to save the current network topology to the **topology.dba** file in the flash memory. After the commander reboots, it uses the **topology.dba** file to restore the network topology.

Examples

Save the current network topology

```
<Sysname> system-view
[Sysname] smartmc topology-save
```

Related commands

display smartmc device-link

smartmc upgrade boot-loader

Use **smartmc upgrade boot-loader** to upgrade the startup software on a list of members or SmartMC groups.

Use **undo smartmc upgrade** delete the startup software upgrade task.

Syntax

smartmc upgrade boot-loader { **group** | **tc** } *list* [**delay** *minutes* | **time** *time*]

smartmc upgrade boot-loader { **group** | **tc** } { *list* { **boot** *boot-filename* **system** *system-filename* | **file** *ipe-filename* } }&<1-40> [**delay** *delay-time* | **time** *time*]

undo smartmc upgrade

Views

System view

Predefined user roles

network-admin

Parameters

group: Specifies the SmartMC groups to be upgraded.

tc: Specifies the members to be upgraded.

list: Specifies a space-separated list of up to 10 member items or SmartMC group items.

- **SmartMC group**—Each item specifies a SmartMC group name, a case-sensitive string of 1 to 31 characters.
- **Member**—Each item specifies a member ID or a range of member IDs in the form of *tc-id1* **to** *tc-id2*. The value for *tc-id2* must be greater than or equal to the value for *tc-id1*. The value range for the *tc-id* argument is 1 to 255.

boot *boot-filename*: Specifies a boot image by its name.

system *system-filename*: Specifies a system image by its name.

file *ipe-filename*: Specifies an IPE file by its name, a case-insensitive string of 5 to 45 characters.

delay *delay-time*: Specifies the upgrade delay time in the range of 1 to 1440 minutes.

time *in-time*: Specifies the upgrade time in the format of *hh:mm*. The value range for the *hh* argument is 0 to 23 hours. The value range for the *mm* argument is 0 to 59 minutes.

Usage guidelines

CAUTION:

Upgrading the startup software might interrupt services. Before upgrading the startup software, make sure no services will be interrupted.

To use this command to upgrade the startup software on members without specifying the upgrade files, you must first perform one of the following tasks:

- Execute the **smartmc tc boot-loader** command to specify the upgrade files for members.
- Execute the **boot-loader** command to specify the upgrade files for a SmartMC group.

A member can perform only one upgrade task at a time.

If you execute this command without specifying the delay time or update time, the members or SmartMC group immediately upgrades the startup software and the upgrade operation cannot be cancelled. If you specify a delay time or upgrade time to perform a scheduled upgrade, the upgrade operation can be cancelled by using the **undo smartmc upgrade** command before it starts.

Examples

Upgrade startup software images **boot.bin** and **sys.bin** on all members in SmartMC groups **test1** and **test2**.

```
<Sysname> system-view
[Sysname] smartmc upgrade boot-loader group test1 test2 boot boot.bin system sys.bin
```

Related commands

boot-loader

startup-configuration

smartmc upgrade startup-configuration

Use **smartmc upgrade startup-configuration** to upgrade the configuration file on a list of members or on all members in SmartMC groups.

Use **undo smartmc upgrade** delete the configuration file upgrade task.

Syntax

smartmc upgrade startup-configuration { **group** | **tc** } *list* [**delay** *minutes* | **time** *time*]

smartmc upgrade startup-configuration group { *list* **file** *cfg-filename* }&<1-40> [**delay** *delay-time* | **time** *time*]

smartmc upgrade startup-configuration tc { *list cfg-filename* }&<1-40> [**delay** *delay-time* | **time** *time*]

undo smartmc upgrade

Views

System view

Predefined user roles

network-admin

Parameters

group: Specifies the SmartMC groups to be upgraded.

tc: Specifies the members to be upgraded.

list: Specifies a space-separated list of up to 10 member items or SmartMC group items.

- **SmartMC group**—Each item specifies a SmartMC group name, a case-sensitive string of 1 to 31 characters.
- **Member**—Each item specifies a member ID or a range of member IDs in the form of *tc-id1* **to** *tc-id2*. The value for *tc-id2* must be greater than or equal to the value for *tc-id1*. The value range for the *tc-id* argument is 1 to 255.

file *cfg-filename*: Specifies a configuration file by its name.

NOTE:

The **file** keyword needs to be entered only in Release 6328 and later.

delay *delay-time*: Specifies the upgrade delay time in the range of 1 to 1440 minutes.

time *in-time*: Specifies the upgrade time in the format of *hh:mm*. The value range for the *hh* argument is 0 to 23 hours. The value range for the *mm* argument is 0 to 59 minutes.

Usage guidelines

CAUTION:

After you update the configuration file, the configuration in the new configuration file will become the running configuration. Before upgrading the configuration file, make sure the contents of the new configuration file are correct.

To use this command to upgrade the configuration file on members without specifying the upgrade file, you must first perform one of the following tasks:

- Execute the **smartmc tc startup-configuration** command to specify the upgrade file for members.
- Execute the **startup-configuration** command to specify the upgrade file for a SmartMC group.

A member can perform only one upgrade task at a time.

If you execute this command without specifying the delay time or update time, the members or SmartMC group immediately upgrades the configuration file and the upgrade operation cannot be cancelled. If you specify a delay time or upgrade time to perform a scheduled upgrade, the upgrade operation can be cancelled by using the **undo smartmc upgrade** command before it starts.

Examples

Upgrade configuration file **startup.cfg** on all members in SmartMC groups **test1** and **test2**.

```
<Sysname> system-view
[Sysname] smartmc upgrade boot-loader group test1 test2 startup.cfg
```

Related commands

boot-loader

startup-configuration

smartmc vlan

Use **smartmc vlan** to create a VLAN for members.

Syntax

smartmc vlan *vlan-id* { **group** *group-name-list* | **tc** *tc-id-list* }

Views

System view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies the VLAN ID in the range of 1 to 4094.

group *group-name-list*: Specifies the SmartMC groups for which the VLAN is created. You can specify a space-separated list of up to 10 SmartMC groups. The group name is a case-sensitive string of 1 to 31 characters.

tc *tc-id-list*: Specifies the members for which the VLAN is created. You can specify a space-separated list of up to 10 member items. Each item specifies a member or a range of members in the form of *tc-id1* **to** *tc-id2*. The value for *tc-id2* must be greater than or equal to the value for *tc-id1*. The value range for the *tc-id* argument is 1 to 255.

Usage guidelines

Execute this command when the network topology is stable. As a best practice, use the **smartmc topology-refresh** command to refresh the network topology before executing this command.

After you execute this command, all access ports on members except the following access ports are assigned to the VLAN:

- Access ports connecting to the commander.
- Access ports connecting to other members.
- Access ports connecting to offline devices. Remove offline devices before configuring this command.

If the VLAN is successfully created but some access ports of a member cannot be assigned to the VLAN, the VLAN memberships of the member is restored to the state before the VLAN is created.

The failure to assign an access port of a member to the created VLAN does not affect the VLAN assignment for other members.

After command execution, you can use the **display smartmc vlan** command to examine the VLAN creation result.

Examples

Create a VLAN for member 1 and member 2.

```
<Sysname> system-view
[Sysname] smartmc vlan 2 tc 1 to 2
As a best practice, execute the display smartmc vlan command to verify that the VLAN has
been created successfully.
```

startup-configuration

Use **startup-configuration** to specify an upgrade configuration file for a SmartMC group .

Use **undo startup-configuration** to restore the default.

Syntax

startup-configuration *cfgfile*

undo startup-configuration

Default

No upgrade configuration file is specified for the SmartMC group.

Views

SmartMC group view

Predefined user roles

network-admin

Parameters

cfgfile: Specifies a configuration file by its name, a string of 5 to 45 characters. The file name must include the **.cfg** extension.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify configuration file **startup.cfg** for SmartMC group **testgroup**.

```
<Sysname> system-view
[Sysname] smartmc group testgroup
[Sysname-smartmc-group-testgroup] startup-configuration startup.cfg
```

Related commands

smartmc group

Contents

WiNet commands

boot-loader file

Use **boot-loader file** to specify the upgrade startup software files for a WiNet group.

Use **undo boot-loader** to restore the default.

Syntax

boot-loader file { *ipe-filename* | **boot** *boot-filename* **system** *system-filename* }

undo boot-loader

Default

No upgrade startup software files are specified for a WiNet group.

Views

WiNet group view

Predefined user roles

network-admin

Parameters

ipe-filename: Specifies an IPE software file by its name, a case-insensitive string of 5 to 45 characters. The file name must include the **.ipe** extension.

boot *boot-filename*: Specifies a boot image file by its name, a case-insensitive string of 5 to 45 characters. The file name must include the **.bin** extension.

system *system-filename*: Specifies a system image file by its name, a case-insensitive string of 5 to 45 characters. The file name must include the **.bin** extension.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify IPE software file **device.ipe** for WiNet group **testgroup**.

```
<Sysname> system-view
[Sysname] winet group testgroup
[Sysname-winet-group-testgroup] boot-loader file device.ipe
```

Related commands

winet group

winet upgrade boot-loader

create batch-file

Use **create batch-file** to create a batch file.

Syntax

create batch-file *batch-file-name*

Default

No batch files exist.

Views

User view

Predefined user roles

network-admin

Parameters

batch-file-name: Specifies the name of the batch file, a case-insensitive string of 1 to 255 characters. If you do not specify a file extension when specifying a file name, the default extension **.cmdset** is used.

Usage guidelines

After executing this command, you will enter the batch edit mode. In this mode, each command occupies a line. When you finish editing all command lines, enter a percent sign (%) to return to user view.

Make sure the command lines that you enter are correct because the system does not verify whether the command lines are correct.

Examples

Create a batch file named **test.cmdset**, and enter the command lines for specifying the device name as **Sysname** and enabling Telnet.

```
<Sysname> create batch-file test.cmdset
Begin to edit batch commands, and quit with the character '%'.
system-view
sysname Sysname
telnet server enable%
<Sysname>
```

Related commands

display winet batch-file status

winet batch-file deploy

display winet backup configuration status

Use **display winet backup configuration status** to display the backup status on members.

Syntax

display winet backup configuration status

Views

Any view

Predefined user roles

network-admin

Usage guidelines

This command displays the status of the ongoing backup task or the most recent backup task if the member is not performing backup.

Examples

Display the backup status on members.

```
<Sysname> display winet backup configuration status
ID     IpAddress        MacAddress          Status       Time
1      192.168.56.30    08d2-38ff-0300      Finished     2017-04-05 11:30:35
2      192.168.56.40    62d2-c21c-0400      Finished     2017-04-05 11:30:40
```

Table 1 Command output

Field	Description
ID	ID of the member.
IpAddress	IP address of the member.
MacAddress	MAC address of the member.
Status	Backup status: • **Waiting**—The member is waiting for configuration backup. • **Processing**—The member is backing up the configuration. • **Finished**—The member has finished backing up the configuration. • **Timeout**—Configuration backup times out. • **Failed**—The member failed to back up the configuration.
Time	Time when the member finished backing up the configuration. If the member has not finished backing up the configuration, this field displays a hyphen (**-**).

Related commands

winet backup configuration

winet backup configuration interval

winet backup configuration max-number

display winet batch-file status

Use **display winet batch-file status** to display the batch file deployment result.

Syntax

display winet batch-file status [**ap** | **last** *number* | **phone**]

Views

Any view

Predefined user roles

network-admin

Parameters

ap: Displays the result of the most recent batch file deployment for ports connected to APs.

last *number*: Specifies a batch file deployment (performed by using the **winet batch-file deploy** command) by its number counting from the most recent batch file deployment. The value range for the *number* argument is 1 to 5.

phone: Displays the result of the most recent batch file deployment for ports connected to IP phones.

Usage guidelines

If you do not specify any parameters, this command displays the result of the most recent batch file deployment performed by using the **winet batch-file deploy** command.

Examples

Display the result of the most recent batch file deployment. In this example, the batch file contains the **display winet configuration** command.

```
<Sysname> display winet batch-file status last 1
TC ID 1
Device MAC : 8a73-60c3-0200
Start Time : 2018-12-24 14:55:39
End   Time : 2018-12-24 14:55:43
Result     :

<Sysname>display winet configuration
Device role              : TC
TM IP                    : 192.168.22.103
TM MAC                   : 8a73-4faa-0100
TM sysname               : Sysname
<Sysname>

TC ID 2
Device MAC : 8a73-6b31-0300
Start Time : 2018-12-24 14:55:43
End   Time : 2018-12-24 14:55:48
Result     :

<Sysname>display winet configuration
Device role              : TC
TM IP                    : 192.168.22.103
TM MAC                   : 8a73-4faa-0100
TM sysname               : Sysname
<Sysname>
```

Table 2 Command output

Field	Description
TC ID	ID of the member.
Device MAC	MAC address of the member.
Start Time	Batch file deployment start time.
End Time	Batch file deployment end time.
Result	Batch file deployment result in details.

Related commands

create batch-file

winet batch-file apply

winet batch-file deploy

display winet configuration

Use **display winet configuration** to display the WiNet configuration.

Syntax

display winet configuration

Views

Any view

Predefined user roles

network-admin

Examples

Display the WiNet configuration on the commander.

Release 6318P01 and earlier:

```
<Sysname> display winet configuration
Device role                          : TM
FTP server IP                        : 192.168.22.103
FTP server username                  : admin
Topology-refresh interval            : 60(s)
Backup startup-configuration interval : N/A
Sync backup number                   : 5
Device status                        : Lack
Some configurations are absent on the TM, such as Telnet or LLDP configuration.
```

Release 6328 and later:

```
<Sysname> display smartmc configuration
Device role                          : TM
File server:
  Type: FTP
  IP address: 192.168.22.103
  Username: admin
  Port: 21
  VPN instance: N/A
  Directory: /FTP
Topology-refresh interval            : 60(s)
Backup startup-configuration interval : N/A
Sync backup number                   : 5
Device status                        : Lack
Some configurations are absent on the TM, such as Telnet or LLDP configuration.
```

Display the commander information on a member.

```
<Sysname> display winet configuration
Device role       : TC
TM IP             : 192.168.22.103
TM MAC            : 8288-468d-0100
TM sysname        : Sysname
```

Table 3 Command output

Field	Description
Device role	Role of the device.
FTP server IP	This field is supported only in Release 6318P01 and earlier. IP address of the FTP server. If no FTP server IP address is configured, this field displays **N/A**.
FTP server username	This field is supported only in Release 6318P01 and earlier. FTP server username. If no username is configured, this field displays **N/A**.
File server	This field is supported only in Release 6328 and later. File server configuration.
Type	This field is supported only in Release 6328 and later. File server type. If no file server is specified, this field displays **N/A**.
IP address	This field is supported only in Release 6328 and later. File server IP address. If no file server is specified, this field displays **N/A**.
Username	This field is supported only in Release 6328 and later. File server username. If no file server is specified, this field displays **N/A**.
Port	This field is supported only in Release 6328 and later. File server port. If no file server is specified, this field displays **N/A**.
VPN instance	This field is supported only in Release 6328 and later. VPN instance to which the file server belongs. If no file server is specified, this field displays **N/A**.
Directory	This field is supported only in Release 6328 and later. Storage directory of files on the file server. If no file server is specified, this field displays **N/A**.
Topology-refresh interval	Topology refresh interval, in seconds.
Backup startup-configuration interval	Automatic configuration file backup interval, in hours. If no interval is set, this field displays **N/A**.
Sync backup number	Number of members that can perform configuration backup at the same time.
Device status	Commander status: • **Normal**. • **Lack**—Lack of configuration, such as NETCONF, Telnet, local user, and LLDP.
TM IP	IP address of the commander. If the member failed to obtain the commander IP address, this field displays **N/A**.
TM MAC	MAC address of the commander, If the member failed to obtain the commander MAC address, this field displays **N/A**.
TM sysname	Name of the commander. If the member failed to obtain the commander name, this field displays **N/A**.
Some configurations are absent on the TM, such as XXX.	This field is available only when the **Device status** field displays **Lack**. Lack of configuration will affect WiNet functions. Please follow the prompt to complete the configuration.

Related commands

`smartmc backup configuration interval`

smartmc backup configuration max-number

smartmc enable

smartmc { **ftp-server** | **sftp-server** }

smartmc topology-refresh interval

display winet device-link

Use **display winet device-link** to display connections between devices in the WiNet network.

Syntax

display winet device-link

Views

Any view

Predefined user roles

network-admin

Examples

Display connections between devices in the WiNet network.

```
<Sysname> display winet device-link
(TM IP)[192.168.56.20]
ID    Hop  LocalPort            LocalIP          PeerPort               PeerIP
0     0    GigabitEthernet1/0/2  192.168.56.20    GigabitEthernet1/0/1   192.168.56.30
1     1    GigabitEthernet1/0/1  192.168.56.30    GigabitEthernet1/0/2   192.168.56.20
1     2    GigabitEthernet1/0/2  192.168.56.30    GigabitEthernet1/0/1   192.168.56.40
2     3    GigabitEthernet1/0/1  192.168.56.40    GigabitEthernet1/0/2   192.168.56.30
```

Table 4 Command output

Field	Description
TM IP	IP address of the commander.
ID	ID of the commander or member.
Hop	Number of hops between the commander and member.
LocalPort	Local port.
LocalIP	IP address of the local device.
PeerPort	Peer port.
PeerIP	IP address of the peer port.

Related commands

winet topology-refresh

winet topology-refresh interval

display winet group

Use **display winet group** to display WiNet group information.

Syntax

display winet group [*group-name*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

Parameters

group-name: Specifies a WiNet group by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this argument, the command displays information about all WiNet groups.

Verbose: Displays detailed WiNet group information. If you do not specify this keyword, the command displays brief WiNet group information.

Examples

Display detailed WiNet group information.

```
<Sysname> display winet group verbose
Group name                    : test
TC count                      : 3
Boot-loader file              :
Startup-configuration file    :
Rule:
 Match Device-type WS5820-WiNet
TCID DeviceType Sysname  IpAddress       MacAddress     Status   Version
1    WS5820     S1       192.168.56.103  0e74-e2fb-0400 Normal   COMWAREV700R001
2    WS5820     S2       192.168.56.102  0e74-ea13-0500 Normal   COMWAREV700R001
3    WS5820     S3       192.168.56.104  0e74-db54-0300 Normal   COMWAREV700R001
```

Table 5 Command output

Field	Description
GroupName	Name of the WiNet group.
TC count	Number of members in the WiNet group.
Boot-loader file	Names of the upgrade startup software files for upgrading the WiNet group. If no upgrade startup software files are specified, this field displays null.
Startup-configuration file	Name of the configuration file for upgrading the WiNet group. If no configuration file is specified, this field displays null.
Rule	Match criteria of the WiNet group.
Match	Match type and its value. The match types include the following: • **Device-type**—Matches members by device type. • **IP-address**—Matches members by IP address. • **MAC-address**—Matches members by MAC address.
TCID	ID of the member.
DeviceType	Device type of the member.
Sysname	Device name of the member.
IpAddress	IP address of the member.
MacAddress	MAC address of the member.

Field	Description
Version	Software version of the member.
Status	Operating status of the member: • **Offline**—The member is offline. • **Normal**—The member is online.

Related commands

match

winet group

display winet replace status

Use **display winet replace status** to display faulty member replacement status.

Syntax

display winet replace status

Views

Any view

Predefined user roles

network-admin

Examples

Display faulty member replacement status.

```
<Sysname> display winet replace status
Faulty ID      : 2
Faulty MAC     : 94e2-cdcb-0600
Replacement ID : 3
Replacement MAC: 2443-5f8c-0200
Mode           : Manual
Status         : Successful
Start time     : 2017-03-21 15:01:31
End time       : 2017-03-21 15:01:40
```

Table 6 Command output

Field	Description
Faulty ID	ID of the faulty member.
Faulty MAC	MAC address of the faulty member.
Replacement ID	ID of the new member.
Replacement MAC	MAC address of the new member.
Mode	Replacement method, which can be **Manual** or **Auto**.
Status	Replacement status: • **Successful**. • **Failed**. • **Replacing**. • **Timeout**.

Field	Description
Start time	Replacement start time
End time	Replacement end time.

Related commands

winet auto-replace enable

winet replace

display winet resource-monitor

Use **display winet resource-monitor** to display resource monitoring information.

Syntax

display winet resource-monitor [**cpu** | **memory** | **temperature**] * [**tc** *tc-id* | **tm**]

Views

Any view

Predefined user roles

network-admin

Parameters

cpu: Displays CPU usage.

memory: Displays memory usage.

temperature: Displays temperature information.

tc *tc-id*: Specify a member by its ID in the range of 1 to 255.

tm: Specify the commander.

Usage guidelines

This command displays CPU usage, memory usage, and temperature information of the commander and members on the commander. For packet dropping information, log in to the Web interface of the commander and access the **WiNet** > **Intelligent O&M** > **Resource monitoring** page. Packet dropping information can be viewed only in Release 6328 and later.

If you do not specify a resource type, this command displays the resource monitoring information of all types.

If you do not specify a member or the commander, this command displays the resource monitoring information for the commander and all members.

Examples

Display the resource monitoring information for member 1.

```
<Sysname> display winet resource-monitor tc 1
TC 1
  Collection time : 2017-07-25 18:02:30
  Slot 1:
    CPU 0 CPU usage: 1%
    Memory usage   : 587076/903332
    Temperature    : 30
```

Table 7 Command output

Field	Description
Collection time	Time when the resource monitoring information was collected.

Related commands

`winet resource-monitor`

display winet resource-monitor configuration

Use **`display winet resource-monitor configuration`** to display resource monitoring configuration.

Syntax

`display winet resource-monitor configuration`

Views

Any view

Predefined user roles

network-admin

Usage guidelines

This command displays CPU usage, memory usage, and temperature monitoring configuration of the commander. In Release 6328 and later, you can view the status of packet dropping monitoring by using the **`display current-configuration | include smartmc`** command.

Examples

Display resource monitoring configuration.

```
<Sysname> display winet resource-monitor configuration
ID  MacAddress      CPU  Memory  Temperature
1   1111-2222-3333  Y    N       N
2   1111-2222-3334  Y    N       N
3   1111-2222-3335  Y    N       N
```

Table 8 Command output

Field	Description
ID	Device ID.
MacAddress	MAC address of the device.
CPU	CPU usage monitoring status: • **Y**—CPU usage monitoring is enabled. • **N**—CPU usage monitoring is disabled. • **-**—The device does not support CPU usage monitoring.
Memory	Memory usage monitoring status: • **Y**—Memory usage monitoring is enabled. • **N**—Memory usage monitoring is disabled. • **-**—The device does not support memory usage monitoring.
Temperature	Temperature monitoring status: • **Y**—Temperature monitoring is enabled. • **N**—Temperature monitoring is disabled.

Field	Description
	• -—The device does not support temperature monitoring.

Related commands

winet resource-monitor

display winet tc

Use **display winet tc** to display member information.

Syntax

display winet tc [*tc-id*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

Parameters

tc-id: Specifies a member by its ID in the range of 1 to 255. If you do not specify a member, this command displays information about all members.

verbose: Displays detailed member information. If you do not specify this keyword, the command displays brief member information.

Examples

Display brief information about all members.

```
<Sysname> display winet tc
TCID DeviceType Sysname  IpAddress       MacAddress     Status   Version
1    WS5820     S1       192.168.22.104  201c-e7c3-0300 Normal   COMWAREV700R001
```

Table 9 Command output

Field	Description
TCID	ID of the member.
DeviceType	Device type of the member.
Sysname	Device name of the member.
IpAddress	IP address of the member.
MacAddress	MAC address of the member.
Status	Operating status of the member: • **Normal**—The member is operating correctly. • **Offline**—The member is offline.
Version	Software version of the member.

Display detailed information about all members.

```
<Sysname> display winet tc verbose
TC ID                        : 1
Adding method                : Manual
Sysname                      : S1
```

```
Model                          : WS5820-WiNet
Device type                    : WS5820-WiNet
SYSOID                         : 1.3.6.1.4.1.25506
MAC address                    : 0e74-e2fb-0400
IP address                     : 192.168.56.103
Boot image                     :
Boot image version             :
System image                   :
System image version           :
Current-configuration file     :
Uptime                         : 2 days, 3 hours, 4 minutes
System CPU usage               : 0%
System memory usage            : 0%
Status                         : Offline
Boot-loader file               :
Startup-configuration file     :
```

Table 10 Command output

Field	Description
TC ID	ID of the member.
Adding method	Method through which the member is added to the WiNet network: • Manual. • Auto.
Sysname	Device name of the member.
Model	Device model of the member.
Device type	Device type of the member.
SYSOID	SYSOID of the member.
MAC address	MAC address of the member.
IP address	IP address of the member.
Boot image	Boot image file that the member runs.
Boot image version	Version of the boot image file.
System image	System image file that the member runs.
System image version	Version of the system image file.
Current-configuration file	Current startup configuration file used by the member.
Uptime	Operation duration of the member.
System CPU usage	CPU usage on the member.
System memory usage	Memory usage on the member.
Status	Operating status of the member: • **Normal**—The member is operating correctly. • **Offline**—The member is offline.
Boot-loader file	Upgrade startup software files.
Startup-configuration file	Upgrade configuration file.

display winet tc log buffer

Use **display winet tc log buffer** to display log information in the log buffer on a member.

Syntax

display winet tc *tc-id* **log buffer** [**module** *module-name* [**mnemonic** *mnemonic-value*]]

Views

Any view

Predefined user roles

network-admin

Parameters

tc-id: Specifies a member by its ID in the range of 1 to 255.

module *module-name*: Specifies a module by its name, a case-insensitive string of 1 to 8 characters. To display module names, use the **info-center source** command (see information center commands in *Network Management and Monitoring Command Reference*).

mnemonic *mnemonic-value*: Specifies a mnemonic, a case-insensitive string of 1 to 32 characters.

Examples

Display the log information for the SHELL module with the SHELL_CMD mnemonic for member 1.

```
<Sysname> display winet tc 1 log buffer module SHELL mnemonic SHELL_CMD
Time     : 2017-07-15 13:51:46
Level    : Informational
Module   : SHELL
Mnemonic : SHELL_CMD
Content  : -Line=con0-IPAddr=**-User=**; Command is qu

Time     : 2017-07-15 13:51:39
Level    : Informational
Module   : SHELL
Mnemonic : SHELL_CMD
Content  : -Line=con0-IPAddr=**-User=**; Command is local-user admin
```

Table 11 Command output

Field	Description
Time	Time when the log was generated.
Level	Log level.

display winet tc log restart

Use **display winet tc log restart** to display the restart log information for a member.

Syntax

display winet tc *tc-id* **log restart**

Views

Any view

Predefined user roles

network-admin

Parameters

tc-id: Specifies a member by its ID in the range of 1 to 255.

Usage guidelines

In addition to saving the logs generated by modules to the log buffer, a member sends restart logs to the commander. The commander creates a restart log buffer for each member to store their restart logs.

The commander stores a maximum of 10 restart logs for each member. The most recent restart log overwrites the oldest one when there are more than 10 restart logs for a member.

You can also use the **display winet tc** *tc-id* **log buffer module** SYSLOG **mnemonic** SYSLOG_RESTART command to display the restart log information.

Examples

Display the restart log information for member 1.

```
<Sysname> display winet tc 1 log restart
Time     : 2017-07-15 13:51:46
Level    : Informational
Module   : SYSLOG
Mnemonic : SYSLOG_RESTART
Content  : System restarted -- H3C Comware Software.
```

Table 12 Command output

Field	Description
Time	Time when the log was generated.
Level	Log level.

Related commands

display winet tc log buffer

display winet upgrade status

Use **display winet upgrade status** to display member upgrade status.

Syntax

display winet upgrade status

Views

Any view

Predefined user roles

network-admin

Examples

Display member upgrade status.

```
<Sysname> display winet upgrade status
```

```
ID    IpAddress         MacAddress      Status      UpdateTime        UpdateFile
1     192.168.56.1      82dd-a434-0200  Finished    Immediately       bootloader.ipe
2     192.168.56.103    5caf-2e5f-0100  Finished    Immediately       bootloader.ipe
```

Table 13 Command output

Field	Description
ID	ID of the member.
MacAddress	MAC address of the member.
IpAddress	IP address of the member.
Status	Upgrade status: • **Waiting**—The member is waiting for downloading the upgrade file. • **Download-failed**—The member failed to download the upgrade file. • **Download-finished**—The member has downloaded the upgrade file. • **Downloading**—The member is downloading the upgrade file. • **Updating**—The member is upgrading. • **Finished**—The member has finished upgrading. • **Failed**—The member failed to upgrade. • **Unknown**—The upgrade status of the member is unknown.
Updated File	Name of the upgrade file.
UpdateTime	Upgrade time: • **Immediately**—Upgrade at once. • **Delay(m)**—Upgrade after the specified delay. • **Time(HH:MM)**—Upgrade at the specified time.

Related commands

`winet upgrade group`

`winet upgrade tc`

display winet vlan

Use **`display winet vlan`** to display VLAN creation results for members.

Syntax

`display winet vlan`

Views

Any view

Predefined user roles

network-admin

Examples

Display VLAN creation results.

```
<Sysname> display winet vlan
ID     IpAddress         MacAddress        Vlan      Status
1      192.168.22.222    703d-15ad-cd02    2         Success
2      192.168.22.3      24ff-2264-0100    2         Success
3      192.168.22.4      24ff-2f74-0200    2         Success
4      192.168.22.223    487a-dac8-29ba    2         Success
```

Table 14 Command output

Field	Description
ID	Member ID.
IpAddress	IP address of the member.
MacAddress	MAC address of the member.
Vlan	VLAN created for the member.
Status	VLAN creation status: • **Processing**—The VLAN is being created. • **Success**—The VLAN has been created successfully. • **Failure. The port xxx is not an access port**—The VLAN fails to be created, because ports connected to non-WiNet devices are not access ports. • **Failure. xxx not exist**—The VLAN fails to be created, because all access ports are connected to WiNet devices.

Related commands

winet vlan

match

Use **match** to set a match criterion to add all matching members to a WiNet group.

Use **undo match** to delete a match criterion.

Syntax

match { **device-type** *device-type* | **ip-address** *ip-address* { *ip-mask-length* | *ip-mask* } | **mac-address** *mac-address mac-mask-length* }

undo match { **device-type** *device-type* | **ip-address** *ip-address* { *ip-mask-length* | *ip-mask* } | **mac-address** *mac-address mac-mask-length* }

Default

No match criterion is set.

Views

WiNet group view

Predefined user roles

network-admin

Parameters

device-type *device-type*: Sets a device type match criterion.

ip-address *ip-address* { *ip-mask-length* | *ip-mask* }: Sets an IP address match criterion. The *ip-address* argument specifies an IP address in dotted decimal notation. The *ip-mask* argument specifies the subnet mask in dotted decimal notation. The *ip-mask-length* argument specifies the subnet mask length in the range of 1 to 32.

mac-address *mac-address mac-mask-length*: Sets a MAC address match criterion. The *mac-address* argument specifies a MAC address in the format of *H-H-H*. The *mac-mask-length* argument specifies the mask length in the range of 1 to 48.

Examples

Create a WiNet group named **a** and add members in subnet 192.168.1.0/24 to the group.

```
<Sysname> system-view
[Sysname] winet group a
[Sysname-winet-group-a] match ip-address 192.168.1.0 24
```

Related commands

winet group

display winet group

winet auto-link-aggregation enable

Use **winet auto-link-aggregation enable** to enable automatic Ethernet link aggregation.

Use **undo winet auto-link-aggregation enable** to disable automatic Ethernet link aggregation.

Syntax

winet auto-link-aggregation enable

undo winet auto-link-aggregation enable

Default

Automatic Ethernet link aggregation is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Automatic Ethernet link aggregation is not performed between the commander and a member.

Enabling or disabling automatic Ethernet link aggregation might cause network flapping, and the members might go offline for a short period of time.

Examples

Enable automatic Ethernet link aggregation.

```
<Sysname> system-view
[Sysname] winet auto-link-aggregation enable
```

winet auto-replace enable

Use **winet auto-replace enable** to enable the automatic faulty member replacement feature.

Use **undo winet auto-replace enable** to disable the automatic faulty member replacement feature.

Syntax

winet auto-replace enable

undo winet auto-replace enable

Default

The automatic faulty member replacement feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

To perform an automatic fault replacement, first enable this feature on the commander, and then perform the following tasks:

1. Install the new member at the location where the faulty member was installed.
2. Connect all cables to the new member.

Make sure the new member and the faulty member have the same neighbor relationship, device model, and IRF member ID.

Examples

Enable the automatic faulty member replacement feature.

```
<Sysname> system-view
[Sysname] winet auto-replace enable
```

Related commands

winet replace

winet backup configuration

Use **winet backup configuration** to manually back up the configuration file on members.

Syntax

winet backup configuration { **group** *group-name-list* | **tc** [*tc-id-list*] }

Views

System view

Predefined user roles

network-admin

Parameters

group *group-name-list*: Specifies a space-separated list of up to 10 WiNet groups. The group name is a case-sensitive string of 1 to 31 characters.

tc *tc-id-list*: Specifies a space-separated list of up to 10 member items. Each item specifies a device or a range of devices in the form of *tc-id1* **to** *tc-id2*. The value for *tc-id2* must be greater than or equal to the value for *tc-id1*. The value range for the *tc-id* argument is 0 to 255, with 0 representing the commander and 1 to 255 representing members. If you do not specify the commander or any members, all devices will perform configuration backup.

Usage guidelines

After you execute this command, the members immediately save the running configuration to the next-startup configuration files and upload the configuration files to the file server.

The backup configuration files are named in the format of *bridge MAC address*_**backup.cfg**.

Examples

Back up the configuration file on member 1, member 2, member 3, and member 4.

```
<Sysname> system-view
[Sysname] winet backup configuration tc 1 to 4
```

Back up the configuration file on all members in WiNet groups **test1**, **test2**, and **test3**.

```
<Sysname> system-view
```

```
[Sysname] winet backup configuration group test1 test2 test3
```

Related commands

display winet configuration

winet backup configuration interval

winet backup configuration max-number

Use **winet backup configuration max-number** to set the maximum number of members that can perform automatic configuration backup at the same time.

Use **undo winet backup configuration max-number** to restore the default.

Syntax

winet backup configuration max-number *max-number*

undo winet backup configuration max-number

Default

A maximum of five members can perform automatic configuration backup at the same time.

Views

System view

Predefined user roles

network-admin

Parameters

max-number: Specifies the maximum number of members that can perform automatic configuration backup at the same time, in the range of 2 to 20.

Usage guidelines

The maximum number of members that can perform automatic configuration at the same time is limited by the performance of the file server. If automatic configuration backup fails, set the maximum number of members to a smaller value.

Examples

Specify that a maximum of 10 members can perform automatic configuration backup at the same time.

```
<Sysname> system-view
[Sysname] winet backup configuration max-number 10
```

Related commands

display winet configuration

winet backup configuration

winet backup configuration interval

winet backup configuration interval

Use **winet backup configuration interval** to enable the automatic configuration file backup feature and set the automatic backup interval.

Use **undo winet backup configuration interval** to restore the default.

Syntax

winet backup configuration interval *interval*

undo winet backup configuration interval

Default

The automatic configuration file backup feature is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the automatic configuration file backup interval in the range of 1 to 720 hours.

Usage guidelines

This command enables the commander and members to back up their configuration files by saving the running configuration to the files and then uploading them to the file server. When you execute this command, the commander and members immediately perform a backup. After that, they back up the configuration files at the specified interval. The backup configuration files are named in the format of *bridge MAC address*_**backup.cfg**.

Examples

Enable the automatic configuration file backup feature and set the backup interval to 24 hours.

```
<Sysname> system-view
[Sysname] winet backup configuration interval 24
```

Related commands

display winet configuration

winet backup configuration

winet batch-file apply

Use **winet batch-file apply** to specify a batch file to deploy to ports connecting APs or IP phones.

Use **undo winet batch-file apply** to remove a batch file specified for ports connecting APs or IP phones.

Syntax

winet batch-file *batch-file-name* **apply** { **ap** | **phone** }

undo winet batch-file apply { **ap** | **phone** }

Default

No batch file is specified for ports connecting APs or IP phones.

Views

System view

Predefined user roles

network-admin

Parameters

batch-file-name: Specifies a batch file by its name, a case-insensitive string of 1 to 255 characters.

ap: Specifies ports connecting APs.

phone: Specifies ports connecting IP phones.

Usage guidelines

With batch file deployment enabled, the commander automatically deploys configurations in the specified batch file to a port connecting an AP or IP phone, simplifying access port configuration.

When the commander first detects the association of an AP or IP phone on a port through LLDP, it deploys the command lines in the specified batch file to the port. If no batch file is specified for the device type, the configurations on the port remain unchanged.

If the AP or IP phone disconnects from the port, the configurations on the port remain. When a new device comes online from the port, configurations used by the port depend on the new device type.

- If the new device is an AP or IP phone and has the same type as the disconnected device, the configurations on the port remain unchanged.
- If the new device is an AP or IP phone but has a different type as the disconnected device, the commander deploys the command lines in the specified batch file to the port. If no batch file is specified for the device type, the configurations on the port remain unchanged.
- If the new device is neither an AP nor an IP phone, the configurations on the port remain unchanged.

To disable the commander from deploying a batch file to ports, remove the specified batch file or execute the **undo winet batch-file-apply enable** command to disable batch file deployment. The **undo winet batch-file-apply enable** command is supported only in Release 6328 and later.

Examples

Specify batch file **ap.cmdset** for ports connecting APs or IP phones.

```
<Sysname> system-view
[Sysname] winet batch-file ap.cmdset apply ap
```

Related commands

create batch-file

winet batch-file-apply enable

winet batch-file deploy

Use **winet batch-file deploy** to deploy bulk command lines to a list of members or WiNet groups.

Syntax

winet batch-file *batch-file-name* **deploy** { **group** *group-name-list* | **tc** **tc**-*id-list* }

Views

System view

Predefined user roles

network-admin

Parameters

batch-file-name: Specifies the name of a batch file, a case-insensitive string of 1 to 255 characters.

group *group-name-list*: Specifies a space-separated list of up to 10 WiNet groups. The group name is a case-sensitive string of 1 to 31 characters.

tc *tc-id-list*: Specifies a space-separated list of up to 10 member items. Each item specifies a member or a range of members in the form of *tc-id1* **to** *tc-id2*. The value for *tc-id2* must be greater than or equal to the value for *tc-id1*. The value range for the *tc-id* argument is 1 to 255.

Examples

Deploy batch file **startup.cmdset** to WiNet group **testgroup**.

```
<Sysname> system-view
[Sysname] winet batch-file startup.cmdset deploy group testgroup
```

Related commands

create batch-file

display winet batch-file status

winet batch-file-apply enable

Use **winet batch-file-apply enable** to enable batch file deployment.

Use **undo winet batch-file-apply enable** to disable batch file deployment.

NOTE:
This command is supported only in Release 6328 and later.

Syntax

winet batch-file-apply enable

undo winet batch-file-apply enable

Default

Batch file deployment is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

With batch file deployment enabled, the commander automatically deploys configurations in the specified batch file to a port connecting an AP or IP phone, simplifying access port configuration. To disable the commander from deploying a batch file to ports, remove the specified batch file or disable batch file deployment.

Examples

Disable batch file deployment.

```
<Sysname> system-view
[Sysname] undo winet batch-file-apply enable
```

Related commands

winet batch-file apply

winet enable

Use **winet enable** to enable WiNet and set the device role.

Use **undo winet enable** to disable WiNet.

Syntax

winet { **tc** | **tm** **username** *username* **password** { **cipher** | **simple** } *string* } **enable**

undo winet enable

Default

WiNet is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

tc: Enables WiNet and sets the device role to member.

tm: Enables WiNet and sets the device role to commander.

username *username*: Specifies a username for the local user, a case-sensitive string of 1 to 55 characters.

password: Specifies a password for the local user.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 63 characters. Its encrypted form is a case-sensitive string of 1 to 117 characters.

Usage guidelines

A WiNet network must have one and only one commander.

To enable WiNet, execute this command on both the commander and members. To configure the other WiNet features, execute associated commands only on the commander.

If you change the role of the commander to member or disable WiNet on the commander, all WiNet settings in its running configuration will be cleared.

WiNet fails to be enabled if ACL resources are insufficient. If ACL resources are insufficient, use the **undo acl** command to delete unnecessary ACLs and then enable WiNet. You can execute the **display acl** command to view ACL configuration and match statistics. For more information about ACLs, see *ACL and QoS Configuration Guide*.

WiNet fails to be enabled if ports 80 and 443 have been used.

If you execute this command multiple times, the most recent configuration takes effect. You can execute the command to change the device role or the password.

Examples

Enable WiNet and set the device role to member.

```
<Sysname> system-view
[Sysname] winet tc enable
```

winet { ftp-server | sftp-server }

Use **winet** { **ftp-server** | **sftp-server** } to configure the file server information.

Use **undo winet** { **ftp-server** | **sftp-server** } to delete the file server information.

Syntax

Release 6318P01 and earlier:

winet ftp-server *server-address* **username** *username* **password** { **cipher** | **simple** } *string*

undo winet ftp-server

Release 6328 and later:

winet { **ftp-server** | **sftp-***server* } { *ipv4-address* | **ipv6** *ipv6-address* } [**port** *port*] [**vpn-instance** *vpn-instance-name*] [**directory** *directory*] **username** *username* **password** { **cipher** | **simple** } *string*

undo winet { **ftp-server** | **sftp-server** }

Default

No file server information is configured.

Views

System view

Predefined user roles

network-admin

Parameters

ftp-server: Specifies an FTP server.

sftp-server: Specifies an SFTP server.

ipv4-address: Specifies the IPv4 address of the file server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the file server.

port *port*: Specifies the port number of the file server, in the range of 1 to 65535. The default pot for an FTP server and an SFTP server is 21 and 22, respectively.

vpn-instance *vpn-instance-name*: Specifies the name of the MPLS L3VPN instance to which the file server belongs, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command considers that the file server is in the public network.

directory *directory*: Specifies the working directory of the file server, a case-insensitive string. By default, the root directory is used.

username *username*: Specifies the file server username, a case-sensitive string of 1 to 55 characters.

password: Specifies the file server password.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 63 characters. Its encrypted form is a case-sensitive string of 1 to 117 characters.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the file server type to FTP, and specify the server IP address, username, and password as 192.168.22.19, **admin**, and **hello12345**, respectively.

```
<Sysname> system-view
[Sysname] winet ftp-server 192.168.22.19 username admin password simple hello12345
```

Related commands

display winet configuration

winet group

Use **winet group** to create a WiNet group and enter its view, or enter the view of an existing WiNet group.

Use **undo winet group** to delete a WiNet group.

Syntax

winet group *group-name*

undo winet group *group-name*

Default

No WiNet groups exist.

Views

System view

Predefined user roles

network-admin

Parameters

group-name: Specifies the name of the WiNet group, a case-sensitive string of 1 to 31 characters.

Usage guidelines

When you perform the following operations, you can specify a WiNet group to apply the operations to all members in the group:

- Startup software upgrade.
- Configuration file upgrade.
- Configuration deployment.

Examples

Create WiNet group **testgroup**.

```
<Sysname> system-view
[Sysname] winet group testgroup
[Sysname-winet-group-testgroup]
```

Related commands

match

winet outbound

Use **winet outbound** to configure an outgoing interface for the WiNet network.

Use **undo winet outbound** to restore the default.

Syntax

winet outbound

undo winet outbound

Default

No interface is used as an outgoing interface, and the WiNet network cannot communicate with outside networks.

Views

Layer 3 Ethernet interface view

VLAN interface view

Predefined user roles

network-admin

Usage guidelines

VLAN interface 1 cannot be used as an outgoing interface, because the WiNet network is established in VLAN 1.

Examples

Configure GigabitEthernet 1/0/1 as an outgoing interface for the WiNet network.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] winet outbound
```

winet resource-monitor

Use **winet resource-monitor** to enable resource monitoring.

Use **undo winet resource-monitor** to disable resource monitoring.

Syntax

winet resource-monitor [**cpu** | **memory** | **packet-drop** | **temperature**] * [**group** *group-name-list* | **tc** { *tc-id-list* | **mac-address** *mac-address* } | **tm**]

undo winet resource-monitor [**cpu** | **memory** | **packet-drop** | **temperature**] * [**group** *group-name-list* | **tc** { *tc-id-list* | **mac-address** *mac-address* } | **tm**]

Default

Resource monitoring is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

cpu: Enables CPU usage monitoring.

memory: Enables memory usage monitoring.

packet-drop: Enables packet dropping monitoring.

NOTE:

The **packet-drop** keyword is supported only in Release 6328 and later.

temperature: Enables temperature monitoring.

group *group-name-list*: Specifies the WiNet groups to monitor. You can specify a space-separated list of up to 10 WiNet groups. The group name is a case-sensitive string of 1 to 31 characters.

tc: Specifies the members to monitor.

tc-id-list: Specifies a space-separated list of up to 10 member items. Each item specifies a member or a range of members in the form of *tc-id1* **to** *tc-id2*. The value for *tc-id2* must be greater than or equal to the value for *tc-id1*. The value range for the *tc-id* argument is 1 to 255.

mac-address *mac-address*: Specifies a member by its MAC address in the format of H-H-H.

tm: Enables resource monitoring on the commander.

Usage guidelines

Packet dropping monitoring monitors packet dropping on members and on interfaces.

If you do not specify a resource type, this command enables resource monitoring for all resource types.

If you do not specify a device to monitor (member or the commander), this command enables resource monitoring on the commander and all members.

Examples

Enable resource monitoring for all resource types on member 1 through member 3.

```
<Sysname> system-view
[Sysname] winet resource-monitor tc 1 to 3
```

Related commands

display winet resource-monitor

winet resource-monitor interval

winet resource-monitor max-age

winet resource-monitor interval

Use **winet resource-monitor interval** to set the interval for the commander to obtain resource monitoring information.

Use **undo winet resource-monitor interval** to restore the default.

Syntax

winet resource-monitor interval *interval*

undo winet resource-monitor interval

Default

The interval for the commander to obtain resource monitoring information is 1 minute.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the interval for the commander to obtain resource monitoring information, in the range of 1 to 60 minutes.

Usage guidelines

For packet dropping monitoring, the specified interval applies only to obtaining of member packet dropping information. Because of the great amount of interface information, the commander obtains interface packet dropping information from members only when Web displaying is requested.

Examples

Set the interval for the commander to obtain resource monitoring information to 5 minutes.

```
<Sysname> system-view
[Sysname] winet resource-monitor interval 5
```

Related commands

display winet resource-monitor

winet resource-monitor

winet resource-monitor max-age

Use **winet resource-monitor max-age** to set the aging time for resource monitoring information.

Use **undo winet resource-monitor max-age** to restore the default.

Syntax

winet resource-monitor max-age *max-age*

undo winet resource-monitor max-age

Default

The aging time for resource monitoring information is 24 hours.

Views

System view

Predefined user roles

network-admin

Parameters

max-age: Specifies the aging time for resource monitoring information, in the range of 1 to 168 hours.

Usage guidelines

For packet dropping monitoring, the specified aging time applies only to member packet dropping information. Each member saves its interface packet dropping information for as long as 30 days.

To view interface packet dropping information, log in to the Web interface of the commander and access the **WiNet** > **Intelligent O&M** > **Resource monitoring** page. You can view information in the past 1 hour, 1 day, or 30 days.

Examples

Set the aging time for resource monitoring information to 1 hour.

```
<Sysname> system-view
[Sysname] winet resource-monitor max-age 1
```

Related commands

display winet resource-monitor

winet resource-monitor

winet replace

Use **winet replace** to manually replace a faulty member.

Syntax

winet replace tc *tc-id1* **faulty-tc** *tc-id2*

Views

System view

Predefined user roles

network-admin

Parameters

tc *tc-id1*: Specifies the ID of the new member, in the range of 1 to 255.

faulty-tc *tc-id2*: Specifies the ID of the faulty member, in the range of 1 to 255.

Usage guidelines

Before you execute this command, perform the following tasks:

1. Install the new member at the location where the faulty member was installed.
2. Connect all cables to the new member.

Make sure the new member and the faulty member have the same neighbor relationship, device model, and IRF member ID.

Examples

Replace faulty member 5 with new member 10.

```
<Sysname> system-view
[Sysname] winet replace tc 10 faulty-tc 5
```

Related commands

display winet replace status

winet auto-replace enable

winet tc boot-loader

Use **winet tc boot-loader** to specify the upgrade startup software files for a member.

Use **undo winet tc boot-loader** to remove the configuration.

Syntax

winet tc *tc-id* **boot-loader** { *ipe-filename* | **boot** *boot-filename* **system** *system-filename* }

undo winet tc *tc-id* **boot-loader**

Views

System view

Predefined user roles

network-admin

Parameters

tc *tc-id*: Specifies a member by its ID in the range of 1 to 255.

ipe-filename: Specifies an IPE software file by its name, a case-insensitive string of 5 to 45 characters. The file name must include the **.ipe** extension.

boot *boot-filename*: Specifies a boot image file by its name, a case-insensitive string of 5 to 45 characters. The file name must include the **.bin** extension.

system *system-filename*: Specifies a system image file by its name, a case-insensitive string of 5 to 45 characters. The file name must include the **.bin** extension.

Examples

Specify upgrade boot image **boot.bin** and upgrade system image **system.bin** for member 1.

```
<Sysname> system-view
[Sysname] winet tc 1 boot-loader boot boot.bin system system.bin
```

Related commands

display winet tc

winet tc device-type

Use **winet tc device-type** to define a member type on the commander.

Use **undo winet tc device-type** to delete a member type.

Syntax

winet tc sysoid *sysoid* **device-type** *device-type*

undo winet tc sysoid *sysoid* **device-type** *device-type*

Views

System view

Predefined user roles

network-admin

Parameters

sysoid *sysoid*: Specifies the SYSOID of a member.

device-type *device-type*: Specifies a member type.

Usage guidelines

A device type can correspond to multiple device models. You can identify different device models with different SYSOIDs by specifying a SYSOID for each device model. The commander identifies member types by SYSOID.

The system predefines the device types for some device models based on SYSOIDs. For device models without predefined device types, you must define their member types by SYSOID manually. If you do not do so, the commander cannot identify the types of such devices.

You cannot modify the predefined device types.

Before defining a device type for a member, you can use the **display winet tc** command to determine whether the member has a predefined one.

- If the member has been predefined with one device type, the **DeviceType** field displays the actual predefined device type.
- If the member does not have a predefined device type, the **DeviceType** field displays **unknown**.

To obtain the SYSOID of a member, use the **display winet tc verbose** command.

Examples

Define a member type by specifying the SYSOID as 1.3.6.1.4.1.25506.1.1588 and the member type as SW.

```
<Sysname> system-view
[Sysname] winet tc sysoid 1.3.6.1.4.1.25506.1.1588 device-type SW
```

winet tc password

Use **winet tc password** to modify the password for the default user (admin) on members.

Use **undo winet tc password** to restore the default.

Syntax

winet tc password [**cipher**] *string*

undo winet tc password

Default

The password for the default user on members is **admin**.

Views

System view

Predefined user roles

network-admin

Parameters

cipher: Specifies a password in encrypted form. If you do not specify this keyword, the command creates a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

NOTE:

The **cipher** keyword is supported only in Release 6328 and later.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 63 characters. Its encrypted form is a case-sensitive string of 33 to 117 characters.

Usage guidelines

During WiNet network establishment, the commander establishes NETCONF sessions to members and adds them to the network. The default username and password on the members for NETCONF session establishment are **admin** and **admin**. To enhance security, you can perform this task to change the password for the default user **admin** of the members after the commander adds the members to the network.

If the default password cannot meet the password complexity requirements on members, you cannot execute the **undo smartmc tc password** command to restore the default.

Do not modify the password for members that are manually added to the WiNet network. If you modify the password for a manually added member, you will not be able to manage that member from the commander.

Examples

Configure default user admin on members to use plaintext password **hello12345**.

```
<Sysname> system-view
[Sysname] smartmc tc password hello12345
```

winet tc startup-configuration

Use **winet tc startup-configuration** to specify the upgrade configuration file for a member.

Use **undo winet tc startup-configuration** to remove the configuration.

Syntax

winet tc *tc-id* **startup-configuration** *cfg-filename*

undo winet tc *tc-id* **startup-configuration**

Views

System view

Predefined user roles

network-admin

Parameters

tc *tc-id*: Specifies a member by its ID in the range of 1 to 255.

cfg-filename: Specifies a configuration file by its name, a case-insensitive string of 5 to 45 characters. The file name must include the **.cfg** extension.

Examples

Specify upgrade configuration file **startup.cfg** for member 1.

```
<Sysname> system-view
[Sysname] winet tc 1 startup-configuration startup.cfg
```

Related commands

display winet tc

winet topology-refresh

Use **winet topology-refresh** to manually refresh the network topology.

Syntax

winet topology-refresh

Views

Any view

Predefined user roles

network-admin

Usage guidelines

To display topology changes, use this command to manually refresh the topology.

Examples

Manually refresh the network topology.

```
<Sysname> winet topology-refresh
```

Related commands

display winet device-link

winet topology-refresh interval

Use **winet topology-refresh interval** to set the automatic network topology refresh interval.

Use **undo winet topology-refresh interval** to restore the default.

Syntax

winet topology-refresh interval *interval*

undo winet topology-refresh interval

Default

The automatic network topology refresh interval is 60 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the automatic network topology refresh interval in the range of 60 to 300 seconds.

Examples

Set the automatic network topology refresh interval to 100 seconds.

```
<Sysname> system-view
[Sysname] winet topology-refresh interval 100
```

Related commands

display winet device-link

winet topology-save

Use **winet topology-save** to save the current network topology.

Syntax

winet topology-save

Views

System view

Predefined user roles

network-admin

Usage guidelines

This task allows you to save the current network topology to the **topology.dba** file in the flash memory. After the commander reboots, it uses the **topology.dba** file to restore the network topology.

Examples

Save the current network topology

```
<Sysname> system-view
[Sysname] winet topology-save
```

Related commands

display winet device-link

winet upgrade boot-loader

Use **winet upgrade boot-loader** to upgrade the startup software on a list of members or WiNet groups.

Use **undo winet upgrade** delete the startup software upgrade task.

Syntax

winet upgrade boot-loader { **group** | **tc** } *list* [**delay** *minutes* | **time** *time*]

winet upgrade boot-loader { **group** | **tc** } { *list* { **boot** *boot-filename* **system** *system-filename* | **file** *ipe-filename* } }&<1-40> [**delay** *delay-time* | **time** *time*]

undo winet upgrade

Views

System view

Predefined user roles

network-admin

Parameters

group: Specifies the WiNet groups to be upgraded.

tc: Specifies the members to be upgraded.

list: Specifies a space-separated list of up to 10 member items or WiNet group items.

- **WiNet group**—Each item specifies a WiNet group name, a case-sensitive string of 1 to 31 characters.
- **Member**—Each item specifies a member ID or a range of member IDs in the form of *tc-id1* **to** *tc-id2*. The value for *tc-id2* must be greater than or equal to the value for *tc-id1*. The value range for the *tc-id* argument is 1 to 255.

boot *boot-filename*: Specifies a boot image by its name.

system *system-filename*: Specifies a system image by its name.

file *ipe-filename*: Specifies an IPE file by its name, a case-insensitive string of 5 to 45 characters.

delay *delay-time*: Specifies the upgrade delay time in the range of 1 to 1440 minutes.

time *in-time*: Specifies the upgrade time in the format of *hh:mm*. The value range for the *hh* argument is 0 to 23 hours. The value range for the *mm* argument is 0 to 59 minutes.

Usage guidelines

CAUTION:

Upgrading the startup software might interrupt services. Before upgrading the startup software, make sure no services will be interrupted.

To use this command to upgrade the startup software on members without specifying the upgrade files, you must first perform one of the following tasks:

- Execute the **winet tc boot-loader** command to specify the upgrade files for members.
- Execute the **boot-loader** command to specify the upgrade files for a WiNet group.

A member can perform only one upgrade task at a time.

If you execute this command without specifying the delay time or update time, the members or WiNet group immediately upgrades the startup software and the upgrade operation cannot be cancelled. If you specify a delay time or upgrade time to perform a scheduled upgrade, the upgrade operation can be cancelled by using the **undo winet upgrade** command before it starts.

Examples

Upgrade startup software images **boot.bin** and **sys.bin** on all members in WiNet groups **test1** and **test2**.

```
<Sysname> system-view
[Sysname] winet upgrade boot-loader group test1 test2 boot boot.bin system sys.bin
```

Related commands

boot-loader

startup-configuration

winet upgrade startup-configuration

Use **winet upgrade startup-configuration** to upgrade the configuration file on a list of members or on all members in WiNet groups.

Use **undo winet upgrade** delete the configuration file upgrade task.

Syntax

winet upgrade startup-configuration { **group** | **tc** } *list* [**delay** *minutes* | **time** *time*]

winet upgrade startup-configuration group { *list* **file** *cfg-filename* }&<1-40> [**delay** *delay-time* | **time** *time*]

winet upgrade startup-configuration tc { **group** | **tc** } { *list* *cfg-filename* }&<1-40> [**delay** *delay-time* | **time** *time*]

undo winet upgrade

Views

System view

Predefined user roles

network-admin

Parameters

group: Specifies the WiNet groups to be upgraded.

tc: Specifies the members to be upgraded.

list: Specifies a space-separated list of up to 10 member items or WiNet group items.

- **WiNet group**—Each item specifies a WiNet group name, a case-sensitive string of 1 to 31 characters.
- **Member**—Each item specifies a member ID or a range of member IDs in the form of *tc-id1* **to** *tc-id2*. The value for *tc-id2* must be greater than or equal to the value for *tc-id1*. The value range for the *tc-id* argument is 1 to 255.

file *cfg-filename*: Specifies a configuration file by its name.

NOTE:

The **file** keyword needs to be entered only in Release 6328 and later.

delay *delay-time*: Specifies the upgrade delay time in the range of 1 to 1440 minutes.

time *in-time*: Specifies the upgrade time in the format of *hh:mm*. The value range for the *hh* argument is 0 to 23 hours. The value range for the *mm* argument is 0 to 59 minutes.

Usage guidelines

CAUTION:

After you update the configuration file, the configuration in the new configuration file will become the running configuration. Before upgrading the configuration file, make sure the contents of the new configuration file are correct.

To use this command to upgrade the configuration file on members without specifying the upgrade file, you must first perform one of the following tasks:

- Execute the **winet tc startup-configuration** command to specify the upgrade file for members.
- Execute the **startup-configuration** command to specify the upgrade file for a WiNet group.

A member can perform only one upgrade task at a time.

If you execute this command without specifying the delay time or update time, the members or WiNet group immediately upgrades the configuration file and the upgrade operation cannot be cancelled. If you specify a delay time or upgrade time to perform a scheduled upgrade, the upgrade operation can be cancelled by using the **undo winet upgrade** command before it starts.

Examples

Upgrade configuration file **startup.cfg** on all members in WiNet groups **test1** and **test2**.

```
<Sysname> system-view
[Sysname] winet upgrade boot-loader group test1 test2 startup.cfg
```

Related commands

boot-loader

startup-configuration

winet vlan

Use **winet vlan** to create a VLAN for members.

Syntax

winet vlan *vlan-id* { **group** *group-name-list* | **tc** *tc-id-list* }

Views

System view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies the VLAN ID in the range of 1 to 4094.

group *group-name-list*: Specifies the WiNet groups for which the VLAN is created. You can specify a space-separated list of up to 10 WiNet groups. The group name is a case-sensitive string of 1 to 31 characters.

tc *tc-id-list*: Specifies the members for which the VLAN is created. You can specify a space-separated list of up to 10 member items. Each item specifies a member or a range of members in the form of *tc-id1* **to** *tc-id2*. The value for *tc-id2* must be greater than or equal to the value for *tc-id1*. The value range for the *tc-id* argument is 1 to 255.

Usage guidelines

Execute this command when the network topology is stable. As a best practice, use the **winet topology-refresh** command to refresh the network topology before executing this command.

After you execute this command, all access ports on members except the following access ports are assigned to the VLAN:

- Access ports connecting to the commander.
- Access ports connecting to other members.
- Access ports connecting to offline devices. Remove offline devices before configuring this command.

If the VLAN is successfully created but some access ports of a member cannot be assigned to the VLAN, the VLAN memberships of the member is restored to the state before the VLAN is created.

The failure to assign an access port of a member to the created VLAN does not affect the VLAN assignment for other members.

After command execution, you can use the **display winet vlan** command to examine the VLAN creation result.

Examples

Create a VLAN for member 1 and member 2.

```
<Sysname> system-view
[Sysname] winet vlan 2 tc 1 to 2
As a best practice, execute the display winet vlan command to verify that the VLAN has
been created successfully.
```

startup-configuration

Use **startup-configuration** to specify an upgrade configuration file for a WiNet group .

Use **undo startup-configuration** to restore the default.

Syntax

startup-configuration *cfgfile*

undo startup-configuration

Default

No upgrade configuration file is specified for the WiNet group.

Views

WiNet group view

Predefined user roles

network-admin

Parameters

cfgfile: Specifies a configuration file by its name, a string of 5 to 45 characters. The file name must include the **.cfg** extension.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify configuration file **startup.cfg** for WiNet group **testgroup**.

```
<Sysname> system-view
[Sysname] winet group testgroup
[Sysname-winet-group-testgroup] startup-configuration startup.cfg
```

Related commands

winet group

Contents

EPA commands

This feature is supported only in Release 6328 and later.

display epa monitor-information

Use **display epa monitor-information** to display endpoint association and disassociation information detected by EPA.

Syntax

display epa monitor-information [**online** | **offline**] [**device** *device-id* | **mac** *mac-address* [**vlan** *vlan-id*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

online: Displays endpoint association information.

offline: Displays endpoint disassociation information.

device *device-id*: Specifies a device by its bridge MAC address in the H-H-H format. In a SmartMC (or WiNet) network, you can specify the bridge MAC address of a member to display only information about endpoints connecting to the member.

mac *mac-address*: Specifies an endpoint by its MAC address in the H-H-H format.

vlan *vlan-id*: Specifies a VLAN by its ID in the range of 1 to 4094. If you do not specify this option, the command displays information in all VLANs.

Usage guidelines

In a SmartMC (or WiNet) network, you can execute this command on the commander or on a member.

- If you execute this command on the commander, you can view information on all devices in the network or information on a specific device.
- If you execute this command on a member, you can view only association events of endpoints connecting to the member.

In a non-SmartMC (or non-WiNet) network, this command displays information only on the device on which the command is executed.

For more information about SmartMC (or WiNet), see *Network Management and Monitoring Configuration Guide*.

Examples

In a SmartMC (or WiNet) network, display endpoint association and disassociation information on the member device with bridge MAC address **3cf5-cc97-772f**.

```
<Sysname> display epa monitor-information device 3cf5-cc97-772f
Local device type   : SmartMC TM
Local device ID     : ae05-0607-eaaa
Endpoint information:
```

```
  Access device ID    MAC address     VLAN    Interface               Status
  3cf5-cc97-772f      0e74-e2fb-0400  11      GE1/0/1                 Online
  3cf5-cc97-772f      5caf-2e5f-0100  11      GE1/0/2                 Offline
```

In a non-SmartMC (or non-WiNet) network, display endpoint association and disassociation information on the current device.

```
<Sysname> display epa monitor-information
Local device type   : Self-managed
Local device ID     : 3cf5-cc97-772e
Endpoint information:
  Access device ID    MAC address     VLAN    Interface               Status
  3cf5-cc97-772e      1cab-34aa-d00e  10      GE1/0/1                 Online
  3cf5-cc97-772e      0000-02b5-ed00  10      GE1/0/2                 Offline
```

Table 1 Command output

Field	Description
Local device type	Local device type. For SmartMC, options include: • **Self-managed**—Indicates a device in a non-SmartMC network. • **SmartMC TM**—Indicates the commander in a SmartMC network. • **SmartMC TC**—Indicates a member in a SmartMC network. For WiNet, options include: • **Self-managed**—Indicates a device in a non-WiNet network. • **WiNet TM**—Indicates the commander in a WiNet network. • **WiNet TC**—Indicates a member in a WiNet network.
Local device ID	Local device ID (bridge MAC address).
Access device ID	ID (bridge MAC address) of the connected device.
MAC address	MAC address of the endpoint.
VLAN	VLAN in which the endpoint resides.
Interface	Interface to which the endpoint is connected.
Status	Endpoint status. Options include: • Online. • Offline.

Related commands

epa monitor-rule

epa monitor-rule

Use **epa monitor-rule** to create an endpoint monitor rule.

Use **undo epa monitor-rule** to remove an endpoint monitor rule.

Syntax

epa monitor-rule [*monitor-rule-id*] **mac** *mac-address* [**mask** *mac-mask*] [**vlan** *vlan-id*]

undo epa monitor-rule { *monitor-rule-id* | **mac** *mac-address* [**mask** *mac-mask*] [**vlan** *vlan-id*] }

Default

No endpoint monitor rules exist.

Views

System view

Predefined user roles

network-admin

Parameters

monitor-rule-id: Specifies the rule ID in the range of 1 to 1024. If you do not specify this argument, the command assigns the smallest available ID to the rule.

mac *mac-address*: Specifies the MAC address of the endpoint to monitor, in the H-H-H format.

mask *mac-mask*: Specifies a MAC address mask, in the H-H-H format.

vlan *vlan-id*: Specifies the VLAN in which the endpoint will be monitored. The *vlan-id* argument represents the VLAN ID in the range of 1 to 4094. If you do not specify this option, the command creates a rule that monitors the endpoint in all VLANs.

Usage guidelines

In a SmartMC (or WiNet) network, you can execute this command only on the commander. The commander will deploy the rule to all members to monitor associations and disassociations of the specified endpoint in the entire network.

In a non-SmartMC (or non-WiNet) network, this command enables the device to monitor associations and disassociations of the specified endpoint only on the device itself.

Examples

Create an endpoint monitor rule to monitor endpoints whose MAC address starts with **0e74** in all VLANs.

```
<Sysname> system-view
[Sysname] epa monitor-rule mac 0e74-e2fb-0400 mask ffff-0000-0000
```

Related commands

display epa monitor-information

epa online-offline-log disable

Use **epa online-offline-log disable** to disable EPA logging.

Use **undo epa online-offline-log disable** to enable EPA logging.

Syntax

epa online-offline-log disable

undo epa online-offline-log disable

Default

EPA logging is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

By default, the EPA module logs endpoint associations and disassociations. If a monitored endpoint comes online or goes offline frequently, the device will generate a large number of log entries. In this case, to avoid affecting device performance, disable EPA logging as a best practice.

Examples

Disable EPA logging.

```
<Sysname> system-view
[Sysname] epa online-offline-log disable
```

Related commands

epa monitor-rule

Telemetry Command Reference

This command reference is applicable to the following switches and software versions:

H3C S5120V2-LI switch series (Release 6308P01 and later)
H3C S3100V3-SI switch series (Release 6309P01 and later)
H3C S5110V2 switch series (Release 6310 and later)
H3C S5110V2-SI switch series (Release 6310 and later)
H3C S5000V3-EI switch series (Release 6310 and later)
H3C S5000V5-EI switch series (Release 6319P01 and later)
H3C S5000E-X switch series (Release 6310 and later)
H3C S5130S-LI switch series (Release 6310 and later)
H3C MS4320V2 switch series (Release 6308P01 and later)
H3C MS4320 switch series (Release 6308P01 and later)
H3C MS4300V2 switch series (Release 6308P01 and later)
H3C MS4200 switch series (Release 6310 and later)
H3C WS5810-WiNet switch series (Release 6308P01 and later)
H3C WS5820-WiNet switch series (Release 6308P01 and later)
H3C WAS6000 switch series (Release 6308P01 and later)
H3C S5000X-EI switch series (Release 6329 and later)
H3C MS4320V3 switch series (Release 6329 and later)
H3C S5120V3-SI switch series (Release 6329 and later)
H3C S5120V3-LI switch series (Release 6329 and later)

New H3C Technologies Co., Ltd.
http://www.h3c.com

Software version: Release 63xx
Document version: 6W105-20230524

Preface

This command reference describes gRPC configuration commands.

This preface includes the following topics about the documentation:

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Documentation feedback

You can e-mail your comments about product documentation to info@h3c.com.

We appreciate your comments.

Contents

gRPC commands

Before you can use gRPC commands, you must install a gRPC feature software image compatible with the device software version. For information about the installation procedure, see software upgrade in *Fundamentals Configuration Guide*.

Generic gRPC commands

display grpc

Use **display grpc** to display gRPC information.

Syntax

display grpc [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

verbose: Display detailed gRPC information. If you do not specify this keyword, the command displays brief gRPC information.

NOTE:

The **verbose** keyword is supported only in Release 6343P08 and later.

Examples

Display brief gRPC information. The sample output is applicable to versions earlier than Release 6343P08.

```
<Sysname> display grpc
gRPC status : enabled.
gRPC port : 50051
gRPC idle-timeout : 3 minutes
Session count: 1.
  Session ID: 1
    User name: test
    Login time:2011-01-05 06:46:43 Idle time : 2 mins 56 s
    Client IP address : 169.254.100.170:40810
    Received RPCs        : 0         Received error RPCs : 0
    Received subscription: 0         Output notifications: 0
```

Table 1 Command output

Field	Description
gRPC status	Status of the gRPC service: • **enabled**—The gRPC service is enabled.

Field	Description
	• **disabled**—The gRPC service is disabled.
gRPC port	Port number for the gRPC service.
gRPC idle-timeout	gRPC session idle timeout timer, in minutes.
Session count	Number of gRPC sessions.
Session ID	ID of a gRPC session.
User name	Username of the gRPC user.
Login time	Date and time when the gRPC user logged in to the device.
Idle time	Amount of time in which the session idle timeout timer will expire. If the value in this field is 0, gRPC sessions will never time out.
Client IP address	IP address and port number of the gRPC client.
Received RPCs	Number of received gRPC requests.
Received error RPCs	Number of received erroneous gRPC requests.
Received subscription	Number of received gRPC subscription requests.
Output notifications	Number of gRPC notifications reported to the collector.

Display brief gRPC information. The sample output is applicable to Release 6343P08 and later.

```
<Sysname> display grpc
gRPC status : Enabled
Current-time: 2020-05-20T04:12:48.119
------------Dial-in mode information------------
gRPC server port: 50052
Session idle-timeout: 10 minutes
Session count: 1
  ID         IP Address:Port                  UserName
   1         192.1.11.254:53030               test
------------Dial-out mode information-----------
Sensor group count: 10
Sensor path count: 70
Destination group count: 5
Destination count: 4
Subscription count: 2
Connection ID: 1
  IP address:Port: 192.1.1.254:11111
   Status: Connected
Connection ID: 2
  Domain name:Port: sample.com(192.1.1.253):50051
   Status: Connected
```

Table 2 Command output

Field	Description
gRPC status	Status of the gRPC service: • **Enabled**—The gRPC service is enabled. • **Disabled**—The gRPC service is disabled.
Current-time	Current system time.

Field	Description
Dial-in mode information	Information about gRPC in dial-in mode.
gRPC server port	Port number for the gRPC service.
Session idle-timeout	gRPC session idle timeout timer, in minutes.
Session count	Number of gRPC sessions.
ID	ID of a gRPC session.
IP Address:Port	IP address and port number of the gRPC client.
UserName	Username of the gRPC user.
Dial-out mode information	Information about gRPC in dial-out mode.
Sensor group count	Number of sensor groups.
Sensor path count	Number of sensor paths.
Destination group count	Number of destination groups.
Destination count	Number of collectors.
Subscription count	Number of subscriptions.
Connection ID	ID of the connection between the device and a collector.
IP address:Port	IP address and service port number of the collector.
Domain name:Port	Domain name and service port number of the collector. This field also displays the first reachable IP address in parentheses for the domain name. If no reachable IP address is available for the domain name, this field displays two hyphens (--) in parentheses.
Status	Status of the channel between the device and the collector: • **Init**—The channel is being initialized. • **Idle**—The channel is idle. • **Connecting**—The channel is being established. • **Connected**—The channel has been established. • **Transient failure**—The channel has failed transiently and is attempting to recover. • **Shutdown**—The channel has been closed because of an issue.

Display detailed gRPC information (available only in Release 6343P08 and later).

```
<Sysname> display grpc verbose
gRPC status : Enabled
Current-time: 2020-05-20T04:12:44.346
------------Dial-in mode information------------
gRPC server port: 50052
Session idle-timeout: 10 minutes
Session count: 1
  Session ID: 1
    User name: test
    Login time:2020-05-19 16:40:16     Idle time : 3 mins 41 s
    Client IP address : 192.1.11.254:53030
    Received RPCs        : 39        Received erroneous RPCs : 6
    Received subscription: 0         Sent notifications: 0
------------Dial-out mode information-----------
Sensor group count: 10
```

```
Sensor path count: 70
Destination group count: 5
Destination count: 4
Subscription count: 1
Subscription s
Source address or interface: not-configure
Sensor group: s
  Sampling interval: N/A
  Sampling type         Effective sampling interval   Sensor path
...
destination-group: d
  Start-time: 2020-05-20T03:38:05.833
  IP:Port: 1.1.1.1:50051
    VPN: N/A
    Periodic sampling statistics:
      Effective count: 272
      Sent successfully: 0                  Failed: 68
    Event-triggered statistics:
      Effective count: 0
      Sent successfully: 0                  Failed: 0
    Queued packets/Queue size: 204/1000
    Dropped: 0
    Last error: Channel(Connecting)
...
```

Table 3 Command output

Field	Description
gRPC status	Status of the gRPC service: • **Enabled**—The gRPC service is enabled. • **Disabled**—The gRPC service is disabled.
Current-time	Current system time.
Dial-in mode information	Information about gRPC in dial-in mode.
gRPC server port	Port number for the gRPC service.
Session idle-timeout	gRPC session idle timeout timer, in minutes.
Session count	Number of gRPC sessions.
Session ID	ID of a gRPC session.
User name	Username of the gRPC user.
Login time	Date and time when the gRPC user logged in to the device.
Idle time	Amount of time in which the session idle timeout timer will expire. If the value in this field is 0, gRPC sessions will never time out.
Client IP address	IP address and port number of the gRPC client.
Received RPCs	Number of received gRPC requests.
Received erroneous RPCs	Number of received erroneous gRPC requests.
Received subscription	Number of received gRPC subscription requests.
Sent notifications	Number of gRPC notifications reported to the collector.

Field	Description
Dial-out mode information	Information about gRPC in dial-out mode.
Sensor group count	Number of sensor groups.
Sensor path count	Number of sensor paths.
Destination group count	Number of destination groups.
Destination count	Number of collectors.
Subscription count	Number of subscriptions.
Subscription	Name of the subscription.
Source address or interface	Source IP address or source interface for packets sent to the collector. This field displays **not-configure** if no source IP address or source interface has been specified.
Sensor group	Name of the sensor group.
Sampling interval	Data sampling interval, in seconds. This field displays **0** for event-triggered sampling.
Sampling type	Data sampling type: • **Event-triggered**—Event-triggered sampling. • **Periodic**—Periodical sampling.
Effective sampling interval	Data sampling interval that takes effect.
Sensor path	Sensor path.
Destination-group	Name of the destination group.
Start-time	Date and time when the gRPC connection was established.
IP:Port	IP address and service port number of the collector (gRPC server).
Domain name:Port	Domain name and service port number of the collector. This field also displays the first reachable IP address in parentheses for the domain name. If no reachable IP address is available for the domain name, this field displays two hyphens (--) in parentheses.
VPN	VPN instance to which the collector belongs. This field displays **N/A** if the collector belongs to the public network.
Periodic sampling statistics	Statistics for periodic sampling.
Event-triggered statistics	Statistics for event-triggered sampling.
Effective count	Number of effective samplings. This counter does not count a sampling if it does not collect any data.
Sent successfully	Number of sent data packets.
Failed	Number of data packets failed to be sent.
Queued packets/Queue size	Number of data packets in queue and the size of the queue.
Dropped	Number of data packets dropped because the queue is full.

Last error	Most recent error:
	• **VPN doesn't exist**—The VPN instance did not exist.
	• **Channel *(reason)***—An error occurred on the gRPC channel. Possible reasons:
	  ○ **Init**—The channel was being initialized.
	  ○ **Idle**—The channel was idle.
	  ○ **Connecting**—The channel was being established.

Field	Description
	○ **Transient failure**—The channel was attempting to recover from a transient failure. ○ **Shutdown**—The channel was closed because of an issue. This field displays two hyphens (**--**) if no errors have occurred.

grpc enable

Use **grpc enable** to enable the gRPC service.

Use **undo grpc enable** to disable the gRPC service.

Syntax

grpc enable

undo grpc enable

Default

The gRPC service is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

If this command fails, use the **display tcp** or **display ipv6 tcp** command to verify whether the gRPC service port number has been used by another feature. If yes, specify a free port as the gRPC service port number and try to enable the gRPC service again.

Examples

Enable the gRPC service.

```
<Sysname> system
[Sysname] grpc enable
```

Related commands

display ipv6 tcp (*Layer 3—IP Services Command Reference*)

display tcp (*Layer 3—IP Services Command Reference*)

grpc port

gRPC dial-in mode commands

grpc idle-timeout

Use **grpc idle-timeout** to set the gRPC session idle timeout timer.

Use **undo grpc idle-timeout** to restore the default.

Syntax

grpc idle-timeout *minutes*

undo grpc idle-timeout

Default

The gRPC session idle timeout timer is 5 minutes.

Views

System view

Predefined user roles

network-admin

Parameters

minutes: Specifies the gRPC session idle timeout timer in minutes, in the range of 0 to 30. To disable gRPC sessions from being timed out, set it to 0.

Usage guidelines

If no gRPC packet exchanges occur on the session between a gRPC and the server before the idle timeout timer expires, the device closes the session.

Examples

Set the gRPC session idle timeout timer to 6 minutes.

```
<Sysname> system
[Sysname] grpc idle-timeout 6
```

grpc port

Use **grpc port** to specify the gRPC service port number.

Use **undo grpc port** to restore the default.

Syntax

grpc port *port-number*

undo grpc port

Default

The gRPC service port number is 50051.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies the gRPC service port number, in the range of 1 to 65535.

Usage guidelines

Changing the gRPC service port number when the gRPC service is enabled reboots the gRPC service and closes gRPC connections to gRPC clients. The gRPC clients must re-initiate the connections.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the gRPC service port number to 50052.

```
<Sysname> system
[Sysname] grpc port 50052
```

Related commands

grpc enable

gRPC dial-out mode commands

destination-group (subscription view)

Use **destination-group** to specify a destination group for a subscription.

Use **undo destination-group** to remove a destination group from a subscription.

Syntax

destination-group *group-name*

undo destination-group *group-name*

Default

A subscription does not have a destination group.

Views

Subscription view

Predefined user roles

network-admin

Parameters

group-name: Specifies a destination group by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

A subscription binds sensor groups to destination groups. Then, the device pushes data from the specified sensors to the collectors.

The specified destination group must have been created by using the **destination-group** command in telemetry view.

You can specify a maximum of five destination groups for a subscription.

Examples

Specify destination group **collector1** for subscription **A**.

```
<Sysname> system-view
[Sysname] telemetry
[Sysname-telemetry] subscription A
[Sysname-telemetry-subscription-A] destination-group collector1
```

Related commands

destination-group (telemetry view)

destination-group (telemetry view)

Use **destination-group** to create a destination group and enter its view, or enter the view of an existing destination group.

Use **undo destination-group** to delete a destination group.

Syntax

destination-group *group-name*

undo destination-group *group-name*

Default

No destination groups exist.

Views

Telemetry view

Predefined user roles

network-admin

Parameters

group-name: Specifies the destination group name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

As a best practice, configure a maximum of five destination groups. Configuring too many destination groups might degrade the system performance.

To delete a destination group that is already used by a subscription, you must remove the destination group from the subscription first.

Examples

Create a destination group named **collector1**.

```
<Sysname> system-view
[Sysname] telemetry
[Sysname-telemetry] destination-group collector1
[Sysname-telemetry-destination-group-collector1]
```

Related commands

destination-group (subscription view)

subscription

domain-name

Use **domain-name** to add the domain name of an IPv4 collector to a destination group.

Use **undo domain-name** to remove the domain name of an IPv4 collector from a destination group.

NOTE:

This command is supported only in Release 6343P08 and later.

Syntax

domain-name *domain-name* [**port** *port-number*] [**vpn-instance** *vpn-instance-name*]

undo domain-name *domain-name* [**port** *port-number*] [**vpn-instance** *vpn-instance-name*]

Default

A destination group does not contain IPv4 collectors.

Views

Destination group view

Predefined user roles

network-admin

Parameters

domain-name: Domain name mapped to the IPv4 address of a collector. It can be a case-insensitive string of 1 to 253 characters and can contain letters, digits, hyphens (-), underscores (_), and dots (.).

port *port-number*: Specifies the service port number on which the collector receives data. The value range is 1 to 65535 and the default is 50051. To have the collector receive data, make sure the specified service port number is the same as the one used on the collector.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the collector belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Make sure the specified VPN instance already exists. If the collector is on the public network, do not specify this option.

Usage guidelines

If you specify collectors by their domain names, you must configure DNS to make sure the device can translate the domain names of the collectors to IPv4 addresses. For more information about DNS, see *Layer 3—IP Services Configuration Guide*.

To view domain name and IP address mappings, use the **display dns host** command. If a domain name maps to multiple IP addresses, the device pushes data to the first reachable IP address.

To add multiple collectors, repeat this command.

A collector is uniquely identified by a three-tuple of domain name, port number, and VPN instance name. One collector must have a different domain name, port number, or VPN instance name than the other collectors.

A destination group can have a maximum of five collectors.

To modify the collector configuration for a destination group that is already used by a subscription, you must remove the destination group from the subscription first.

Examples

Add the IPv4 collector at sample.com to destination group collector1.

```
<Sysname> system-view
[Sysname] telemetry
[Sysname-telemetry] destination-group collector1
[Sysname-telemetry-destination-group-collector1] domain-name sample.com
```

Related commands

destination-group (subscription view)

subscription

display dns host (*Layer 3—IP Services Command Reference*)

ipv4-address

Use **ipv4-address** to add an IPv4 collector to a destination group.

Use **undo ipv4-address** to remove an IPv4 collector from a destination group.

Syntax

ipv4-address *ipv4-address* [**port** *port-number*]

undo ipv4-address *ipv4-address* [**port** *port-number*]

Default

A destination group does not have IPv4 collectors.

Views

Destination group view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies the IPv4 address of the collector.

port *port-number*: Specifies the listening port of the collector, in the range of 1 to 65535. The default is 50051.

Usage guidelines

To add multiple collectors to a destination group, execute this command multiple times.

One collector must have a different address, port, or VPN instance than the other collectors.

You can specify a maximum of five collectors for a destination group.

To modify the collector configuration for a destination group that is already used by a subscription, you must remove the destination group from the subscription first.

Examples

Add a collector that uses IPv4 address 192.168.21.21 and the default port number to destination group **collector1**.

```
<Sysname> system-view
[Sysname] telemetry
[Sysname-telemetry] destination-group collector1
[Sysname-telemetry-destination-group-collector1] ipv4-address 192.168.21.21
```

Related commands

destination-group (subscription view)

subscription

ipv6-address

Use **ipv6-address** to add an IPv6 collector to a destination group.

Use **undo ipv6-address** to remove an IPv6 collector from a destination group.

Syntax

ipv6-address *ipv6-address* [**port** *port-number*]

undo ipv6-address *ipv6-address* [**port** *port-number*]

Default

A destination group does not have IPv6 collectors.

Views

Destination group view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the IPv6 address of the collector.

port *port-number*: Specifies the listening port of the collector, in the range of 1 to 65535. The default is 50051.

Usage guidelines

To add multiple collectors to a destination group, execute this command multiple times.

One collector must have a different address, port, or VPN instance than the other collectors.

You can specify a maximum of five collectors for a destination group.

To modify the collector configuration for a destination group that is already used by a subscription, you must remove the destination group from the subscription first.

Examples

Add a collector that uses IPv6 address 1: : 1 and the default port number to destination group **collector1**.

```
<Sysname> system-view
[Sysname] telemetry
[Sysname-telemetry] destination-group collector1
[Sysname-telemetry-destination-group-collector1] ipv6-address 1: : 1
```

Related commands

destination-group (subscription view)

subscription

ipv6 domain-name

Use **ipv6 domain-name** to add the domain name of an IPv6 collector to a destination group.

Use **undo ipv6 domain-name** to remove the domain name of an IPv6 collector from a destination group.

NOTE:
This command is supported only in Release 6343P08 and later.

Syntax

ipv6 domain-name *domain-name* [**port** *port-number*] [**vpn-instance** *vpn-instance-name*]

undo ipv6 domain-name *domain-name* [**port** *port-number*] [**vpn-instance** *vpn-instance-name*]

Default

A destination group does not contain IPv6 collectors.

Views

Destination group view

Predefined user roles

network-admin

Parameters

domain-name: Domain name mapped to the IPv6 address of a collector. It can be a case-insensitive string of 1 to 253 characters and can contain letters, digits, hyphens (-), underscores (_), and dots (.).

port *port-number*: Specifies the service port number on which the collector receives data. The value range is 1 to 65535 and the default is 50051. To have the collector receive data, make sure the specified service port number is the same as the one used on the collector.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the collector belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Make sure the specified VPN instance already exists. If the collector is on the public network, do not specify this option.

Usage guidelines

If you specify IPv6 collectors by their domain names, you must configure DNS to make sure the device can translate the domain names of the collectors to IPv6 addresses. For more information about DNS, see *Layer 3—IP Services Configuration Guide*.

To view domain name and IP address mappings, use the **display dns host** command. If a domain name maps to multiple IP addresses, the device pushes data to the first reachable IP address.

To add multiple collectors, repeat this command.

A collector is uniquely identified by a three-tuple of domain name, port number, and VPN instance name. One collector must have a different domain name, port number, or VPN instance name than the other collectors.

A destination group can have a maximum of five collectors.

To modify the collector configuration for a destination group that is already used by a subscription, you must remove the destination group from the subscription first.

Examples

Add the IPv6 collector at sample.com to destination group collector1.

```
<Sysname> system-view
[Sysname] telemetry
[Sysname-telemetry] destination-group collector1
[Sysname-telemetry-destination-group-collector1] ipv6 domain-name sample.com
```

Related commands

destination-group (subscription view)

subscription

display dns host (*Layer 3—IP Services Command Reference*)

sensor path

Use **sensor path** to configure a sensor path.

Use **undo sensor path** to delete a sensor path.

Syntax

sensor path *path*

undo sensor path *path*

Default

No sensor paths exist.

Views

Sensor group view

Predefined user roles

network-admin

Parameters

path: Specifies a data path. For information about the available paths, enter a question mark (?) in the position of this argument.

Usage guidelines

To configure multiple sensor paths, execute this command multiple times.

The device supports a maximum of 128 sensor paths.

If the device does not support the specified sensor path, the command displays an error message.

To modify the sensor path configuration for a sensor group that is already used by a subscription, you must remove the sensor group from the subscription first.

Examples

Configure sensor path **ifmgr/devicecapabilities/** for sensor group **test**.

```
<Sysname> system-view
[Sysname] telemetry
[Sysname-telemetry] sensor-group test
[Sysname-telemetry-sensor-group-test] sensor path ifmgr/devicecapabilities/
```

Related commands

sensor-group (subscription view)

subscription

sensor-group (subscription view)

Use **sensor-group** to specify a sensor group for a subscription.

Use **undo sensor-group** to remove a sensor group from a subscription.

Syntax

sensor-group *group-name* [**sample-interval** *interval*]

undo sensor-group *group-name*

Default

A subscription does not have a sensor group.

Views

Subscription view

Predefined user roles

network-admin

Parameters

group-name: Specifies a sensor group by its name, a case-sensitive string of 1 to 31 characters.

sample-interval *interval*: Specifies the data sampling interval in seconds. The value range is 1 to 86400.

Usage guidelines

Specify the **sample-interval** *interval* option for periodic sensor paths and only for periodic sensor paths.

- If you specify the option for event-triggered sensor paths, the sensor paths do not take effect.
- If you do not specify the option for periodic sensor paths, the device does not sample or push data.

The specified sensor group must have been created by using the **sensor-group** command in telemetry view.

Examples

Specify sensor group **test** for subscription **A**. Set the data sampling interval to 10 seconds.

```
<Sysname> system-view
[Sysname] telemetry
[Device-telemetry] subscription A
[Device-telemetry-subscription-A] sensor-group test sample-interval 10
```

Related commands

sensor path

sensor-group (telemetry view)

sensor-group (telemetry view)

Use **sensor-group** to create a sensor group and enter its view, or enter the view of an existing sensor group.

Use **undo sensor-group** to delete a sensor group.

Syntax

sensor-group *group-name*

undo sensor-group *group-name*

Default

No sensor groups exist.

Views

Telemetry view

Predefined user roles

network-admin

Parameters

group-name: Specifies the sensor group name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

The device supports a maximum of 32 sensor groups.

To delete a sensor group that is already used by a subscription, you must remove the sensor group from the subscription first.

Examples

Create a sensor group named **test**.

```
<Sysname> system-view
[Sysname] telemetry
```

```
[Sysname-telemetry] sensor-group test
[Sysname-telemetry-sensor-group-test]
```

Related commands

sensor-group (subscription view)

subscription

source-address

Use **source-address** to specify the source IP address for packets sent to collectors.

Use **undo source-address** to restore the default.

Syntax

source-address { *ipv4-address* | **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }

undo source-address

Default

The device uses the primary IPv4 address of the output interface for the route to the collectors as the source address.

Views

Subscription view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies an IPv4 address.

interface *interface-type interface-number*: Specifies an interface by its type and number. In the current software version, you must specify a loopback interface. The device will use the interface's primary IPv4 address as the source address. If the interface does not have a primary IPv4 address, the device uses the primary IPv4 address of the output interface for the route to the collectors.

ipv6 *ipv6-address*: Specifies an IPv6 address.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Changing the source IP address for packets sent to collectors causes the device to re-establish the connection to the gRPC server.

Examples

Specify the source IPv4 address of 169.254.1.1 for packets sent to collectors.

```
<Sysname> system-view
[Sysname] telemetry
[Sysname-telemetry] subscription A
[Sysname-telemetry-subscription-A] source-address 169.254.1.1
```

subscription

Use **subscription** to create a subscription and enter its view, or enter the view of an existing subscription.

Use **undo sensor-group** to delete a subscription.

Syntax

subscription *subscription-name*

undo subscription *subscription-name*

Default

No subscription groups exist.

Views

Telemetry view

Predefined user roles

network-admin

Parameters

subscription-name: Specifies the subscription name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

The device supports a maximum of 10 subscriptions.

Examples

Configure a subscription named **A**.

```
<Sysname> system-view
[Sysname] telemetry
[Sysname-telemetry] subscription A
[Sysname-telemetry-subscription-A]
```

Related commands

destination-group (subscription view)

sensor-group (subscription view)

telemetry

Use **telemetry** to enter telemetry view.

Syntax

telemetry

Views

System view

Predefined user roles

network-admin

Usage guidelines

In telemetry view, you can configure telemetry parameters.

Examples

Enter telemetry view.

```
<Sysname> system-view
[Sysname] telemetry
[Sysname-telemetry]
```

OpenFlow Command Reference

This command reference is applicable to the following switches and software versions:

H3C S5120V2-LI switch series (Release 6308P01 and later)
H3C S3100V3-SI switch series (Release 6309P01 and later)
H3C S5110V2 switch series (Release 6310 and later)
H3C S5110V2-SI switch series (Release 6310 and later)
H3C S5000V3-EI switch series (Release 6310 and later)
H3C S5000V5-EI switch series (Release 6319P01 and later)
H3C S5000E-X switch series (Release 6310 and later)
H3C S5130S-LI switch series (Release 6310 and later)
H3C MS4320V2 switch series (Release 6308P01 and later)
H3C MS4320 switch series (Release 6308P01 and later)
H3C MS4300V2 switch series (Release 6308P01 and later)
H3C MS4200 switch series (Release 6310 and later)
H3C WS5810-WiNet switch series (Release 6308P01 and later)
H3C WS5820-WiNet switch series (Release 6308P01 and later)
H3C WAS6000 switch series (Release 6308P01 and later)
H3C S5000X-EI switch series (Release 6329 and later)
H3C MS4320V3 switch series (Release 6329 and later)
H3C S5120V3-SI switch series (Release 6329 and later)
H3C S5120V3-LI switch series (Release 6329 and later)

New H3C Technologies Co., Ltd.
http://www.h3c.com

Software version: Release 63xx
Document version: 6W105-20230524

Preface

This command reference describes OpenFlow configuration commands.

This preface includes the following topics about the documentation:

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Documentation feedback

You can e-mail your comments about product documentation to info@h3c.com.

We appreciate your comments.

Contents

OpenFlow commands

active instance

Use **active instance** to activate an OpenFlow instance.

Use **undo active instance** to deactivate an OpenFlow instance.

Syntax

active instance

undo active instance

Default

An OpenFlow instance is not activated.

Views

OpenFlow instance view

Predefined user roles

network-admin

Usage guidelines

After an OpenFlow instance is created or modified, use this command to activate or reactivate the instance to make the instance take effect. After an OpenFlow instance is reactivated, it disconnects from all controllers, clears the deployed flow tables, updates the capability set, and then reconnects to controllers.

Examples

Activate OpenFlow instance 1.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] active instance
```

classification

Use **classification** to configure the OpenFlow instance mode.

Use **undo classification** to restore the default.

Syntax

classification vlan *vlan-id* [**mask** *vlan-mask*] [**loosen**]

undo classification

Default

The OpenFlow instance mode is not configured.

Views

OpenFlow instance view

Predefined user roles

network-admin

Parameters

vlan: Specifies the VLAN mode.

vlan-id: Specifies a VLAN ID in the range of 1 to 4094.

vlan-mask: Specifies a VLAN mask in the range of 0 to 4095. The default value is 4095.

loosen: Specifies the loosen mode. If the loosen mode is used, a port belongs to the OpenFlow instance when VLANs associated with the OpenFlow instance overlap with the port's allowed VLANs. If you do not specify the loosen mode, a port belongs to an OpenFlow instance only when VLANs associated with the OpenFlow instance are within the port's allowed VLAN list.

Usage guidelines

The VLANs to be associated are calculated by a bitwise AND operation on the specified VLAN ID and mask. The VLAN mask supports non-contiguous 1s and ignores all 0 bits. To view the associated VLANs, use the **display openflow instance** command.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Enable the VLAN mode for OpenFlow instance 1 and associate OpenFlow instance 1 with VLANs determined by VLAN ID 255 and VLAN mask 7.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] classification vlan 255 mask 7
```

Related commands

display openflow instance

controller address

Use **controller address** to specify a controller for an OpenFlow switch and configure the main connection to the controller.

Use **undo controller address** to delete the main connection to the specified controller.

Syntax

controller *controller-id* **address** { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**port** *port-number*] [**local address** { **ip** *local-ipv4-address* | **ipv6** *local-ipv6-address* } [**port** *local-port-number*]] [**ssl** *ssl-policy-name*] [**vrf** *vrf-name*]

undo controller *controller-id* **address**

Default

An OpenFlow instance does not have a main connection to a controller.

Views

OpenFlow instance view

Predefined user roles

network-admin

Parameters

controller-id: Specifies a controller by its ID in the range of 0 to 63.

ip *ipv4-address*: Specifies the IPv4 address of the controller.

ipv6 *ipv6-address*: Specifies the IPv6 address of the controller.

port *port-number*: Sets the port number used by the controller to establish TCP connections to the OpenFlow switch. The value range for the port number is 1 to 65535. The default value is 6633.

local address: Specifies the source IP address used to establish TCP connections to the controller. When multiple routes are available between a controller and a switch, you can use this keyword to configure a source IP address for the switch. When the switch restarts or an active/standby switchover occurs, the switch can use the original route to reconnect to the controller without selecting a new route.

ip *local-ipv4-address*: Specifies the source IPv4 address.

ipv6 *local-ipv6-address*: Specifies the source IPv6 address.

port *local-port-number*: Specifies the source port number in the range of 1 to 65535. If you do not specify this option, the system automatically assigns a source port number for establishing the main connection to the controller.

ssl *ssl-policy-name*: Specifies the SSL client policy that the controller uses to authenticate the OpenFlow switch. The *ssl-policy-name* argument is a case-insensitive string of 1 to 31 characters. You must configure a separate SSL client policy for the main connection to each controller.

Usage guidelines

You can specify multiple controllers for an OpenFlow switch. The OpenFlow channel between the OpenFlow switch and each controller can have only one main connection.

The OpenFlow switch uses the main connection to a controller to exchange control messages with the controller to perform the following operations:

- Receive flow table entries or data from the controller.
- Report information to the controller.

As a best practice, configure a unicast IP address for a controller. An OpenFlow switch might fail to establish a connection with the controller that does not use a unicast IP address.

The main connection must be a reliable TCP or SSL connection. The OpenFlow switch uses the main connection to a controller to exchange control messages with the controller to perform the following operations:

- Receive flow table entries or data from the controller.
- Report information to the controller.

Examples

Specify controller 1 for OpenFlow instance 1. The controller's IP address is 1.1.1.1 and the port number is 6666.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] controller 1 address ip 1.1.1.1 port 6666
```

controller auxiliary

Use **controller auxiliary** to specify a controller for an OpenFlow switch and configure an auxiliary connection to the controller.

Use **undo controller auxiliary** to delete the specified auxiliary connection to the specified controller.

Syntax

controller *controller-id* **auxiliary** *auxiliary-id* **transport** { **tcp** | **udp** | **ssl** *ssl-policy-name* } [**address** { **ip** *ipv4-address* | **ipv6** *ipv6-address* }] [**port** *port-number*]

undo controller *id* **auxiliary** *auxiliary-id*

Default

An OpenFlow instance does not have auxiliary connections to a controller.

Views

OpenFlow instance view

Predefined user roles

network-admin

Parameters

controller-id: Specifies a controller by its ID in the range of 0 to 63.

auxiliary *auxiliary-id*: Specifies an auxiliary connection ID in the range of 1 to 255.

transport: Specifies the transport layer protocol.

tcp: Specifies TCP connections.

udp: Specifies UDP connections.

ssl *ssl-policy-name*: Specifies the SSL client policy that the controller uses to authenticate the OpenFlow switch. The *ssl-policy-name* argument is a case-insensitive string of 1 to 31 characters.

ip *ipv4-address*: Specifies the IPv4 address of the controller.

ipv6 *ipv6-address*: Specifies the IPv6 address of the controller.

port *port-number*: Sets the port number used to establish TCP connections to the controller. The value range for the port number is 1 to 65535. The default value is 6633.

Usage guidelines

Auxiliary connections are used to improve the communication performance between the controller and OpenFlow switches.

For an auxiliary connection to be successfully established, make sure the configuration of the auxiliary connection does not conflict with the configuration of the main connection.

An auxiliary connection can have a different destination IP address and port number than the main connection. If no destination IP address and port number are specified, the auxiliary connection uses the destination IP address and port number configured for the main connection.

Examples

Specify controller 1 for OpenFlow instance 1 and configure auxiliary connection 1 to the controller.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] controller 10 auxiliary 1 transport tcp
```

controller connect interval

Use **controller connect interval** to set the reconnection interval.

Use **undo controller connect interval** to restore the default.

Syntax

controller connect interval *interval*

undo controller connect interval

Default

The reconnection interval is 60 seconds.

Views

OpenFlow instance view

Predefined user roles

network-admin

Parameters

interval: Specifies the reconnection interval in the range of 10 to 120 seconds.

Examples

Set the reconnection interval to 10 seconds for OpenFlow instance 1.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] controller connect interval 10
```

controller echo-request interval

Use **controller echo-request interval** to set the connection detection interval for an OpenFlow switch.

Use **undo controller echo-request interval** to restore the default.

Syntax

controller echo-request interval *interval*

undo controller echo-request interval

Default

The connection detection interval is 5 seconds for an OpenFlow switch.

Views

OpenFlow instance view

Predefined user roles

network-admin

Parameters

interval: Specifies the connection detection interval in the range of 1 to 10 seconds.

Examples

Set the connection detection interval to 10 seconds for OpenFlow instance 1.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] controller echo-request interval 10
```

controller mode

Use **controller mode** to set the controller connection mode for an OpenFlow instance.

Use **undo controller mode** to restore the default.

Syntax

controller mode { **multiple** | **single** }

undo controller mode

Default

The controller connection mode is **multiple**.

Views

OpenFlow instance view

Predefined user roles

network-admin

Parameters

multiple: Specifies the **multiple** mode. In **multiple** mode, the OpenFlow switch simultaneously connects to all controllers. If one or more controllers become invalid or disconnected, the OpenFlow switch continues to exchange messages with the rest of the controllers.

single: Specifies the **single** mode. In **single** mode, the OpenFlow switch connects to only one controller at a time. When communication with the current controller fails, the OpenFlow instance connects to the controller with the lowest ID among the rest controllers.

Examples

Set all controllers of OpenFlow instance 1 to operate in **single** mode.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] controller mode single
```

datapath-id

Use **datapath-id** to set the datapath ID for an OpenFlow instance.

Use **undo datapath-id** to restore the default.

Syntax

datapath-id *id*

undo datapath-id

Default

The datapath ID of an OpenFlow instance contains the instance ID and the bridge MAC address of the device. The lower 16 bits are the instance ID and the upper 48 bits are the bridge MAC address of the device.

Views

OpenFlow instance view

Predefined user roles

network-admin

Parameters

id: Specifies the datapath ID for the OpenFlow instance, in the range of 1 to ffffffffffffffff in hexadecimal format.

Usage guidelines

The datapath ID uniquely identifies an OpenFlow instance.

Examples

Set the datapath ID to **123456** for OpenFlow instance 1.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] datapath-id 123456
```

default table-miss permit

Use **default table-miss permit** to configure the default action of table-miss flow entries to forward packets to the normal pipeline.

Use **undo default table-miss permit** to restore the default.

Syntax

default table-miss permit

undo default table-miss permit

Default

The default action of a table-miss flow entry is to drop packets.

Views

OpenFlow instance view

Predefined user roles

network-admin

Examples

Configure the default action of table-miss flow entries to forward packets to the normal pipeline.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] default table-miss permit
```

description

Use **description** to configure a description for an OpenFlow instance.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

An OpenFlow instance does not have a description.

Views

OpenFlow instance view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 255 characters.

Examples

Configure the description as **test-desc** for OpenFlow instance 1.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] description test-desc
```

display openflow

Use **display openflow** to display controller information for an OpenFlow instance.

Syntax

display openflow instance *instance-id* { **controller** [*controller-id*] | **listened** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

instance-id: Specifies an OpenFlow instance by its ID in the range of 1 to 4094.

controller-id: Specifies a controller by its ID in the range of 0 to 63. If you do not specify a controller ID, this command displays information about all controllers for an OpenFlow instance.

listened: Specifies the controllers acting as SSL clients to which the OpenFlow instance connects as an SSL server.

Examples

Display controller information for OpenFlow instance 100.

```
<Sysname> display openflow instance 100 controller
Instance 1 controller information:
 Reconnect interval : 60 (s)
 Echo interval      : 5  (s)

 Controller ID           : 1
 Controller IP address   : 192.168.49.49
 Controller port         : 6633
 Local IP address        : 192.0.0.1
 Local port              : 5566
 Controller role         : Equal
 Connect type            : TCP
 Connect state           : Established
 Packets sent            : 9
 Packets received        : 9
 SSL policy              : --
 VRF name                : --
```

Table 1 Command output

Field	Description
Reconnect interval	Reconnection interval (in seconds) for an OpenFlow instance to reconnect to all controllers.
Echo interval	Connection detection interval (in seconds) at which an OpenFlow instance sends an echo request message to all controllers.
Controller IP address	IP address of the controller.
Controller port	TCP port number of the controller.
Local IP address	Source IP address of the controller that is connected to the OpenFlow instance.
Local port	Source TCP port number of the current controller.
Controller role	Role of the controller: • **Equal**—The controller has the same mode as other controllers that are specified for the OpenFlow instance. • **Master**—The controller is the master controller for the OpenFlow instance. • **Slave**—The controller is a subordinate controller for the OpenFlow instance. If the controller is not configured with any role, this field displays two hyphens (**--**).
Connect type	Type of the connection between the OpenFlow instance and the controller: **TCP** or **SSL**.
Connect state	State of the connection between the OpenFlow instance and the controller: **Idle** or **Established**.
Packets sent	Number of packets that have been sent to the controller.
Packets received	Number of packets that have been received from the controller.
SSL policy	Name of the SSL client policy used for SSL connections. If no SSL client policy is configured, this field displays two hyphens (**--**).
VRF name	Name of the MPLS L3VPN to which the controller belongs. If no MPLS L3VPN instance is configured, this field displays two hyphens (**--**). This field is not supported in the current software version.

display openflow auxiliary

Use **display openflow auxiliary** to display auxiliary connection information for an OpenFlow instance.

Syntax

display openflow instance *instance-id* **auxiliary** [*controller-id* [**auxiliary** *auxiliary-id*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

instance-id: Specifies an OpenFlow instance by its ID in the range of 1 to 4094.

controller-id: Specifies a controller by its ID in the range of 0 to 63.

auxiliary *auxiliary-id*: Specifies an auxiliary connection by its ID in the range of 1 to 255.

Examples

Display auxiliary connection information for OpenFlow instance 100.

```
<Sysname> display openflow instance 100 auxiliary
Controller ID: 1    Auxiliary connection number: 2
 Auxiliary connection ID : 1
  Controller IP address  : 192.168.49.48
  Controller port        : 6633
  Connect type           : TCP
  Connect state          : Established
  Packets sent           : 9
  Packets received       : 9
  SSL policy             : --

 Auxiliary connection ID : 2
  Controller IP address  : 192.168.49.49
   Controller port       : 6633
   Connect type          : TCP
   Connect state         : Established
   Packets sent          : 9
   Packets received      : 9
   SSL policy            : --
```

Table 2 Command output

Field	Description
Auxiliary connection number	Total number of auxiliary connections.
Auxiliary connection ID	ID of an auxiliary connection.
Controller IP address	IP address of the controller.
Controller port	TCP port number of the controller.
Connect type	Type of the connection between the OpenFlow instance and the controller: **TCP UDP**, or **SSL**.
Connect state	State of the connection between the OpenFlow instance and the controller: **Idle** or **Established**.
Packets sent	Number of packets that have been sent to the controller.
Packets received	Number of packets that have been received from the controller.
SSL policy	Name of the SSL client policy used for SSL connections. If no SSL client policy is configured, this field displays two hyphens (**--**).

display openflow flow-table

Use **display openflow flow-table** to display flow table information for an OpenFlow instance.

Syntax

display openflow instance *instance-id* **flow-table** [*table-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

instance-id: Specifies an OpenFlow instance by its ID in the range of 1 to 4094.

table-id: Specifies a flow table by its ID in the range of 0 to 254. If you do not specify a flow table ID, the command displays information about all flow tables for the specified OpenFlow instance.

Examples

Display information about all flow tables for OpenFlow instance 100.

```
<Sysname> display openflow instance 100 flow-table
Instance 100 flow table information:

Table 0 information:
 Table type: MAC-IP, flow entry count: 1, total flow entry count: 2

MissRule (default) flow entry information:
 cookie: 0x0, priority: 0, hard time: 0, idle time: 0, flags: reset_counts
 |no_pkt_counts|no_byte_counts, byte count: --, packet count: --
 Create time: 09:39:42 10/24/2017, Last modified time: 09:39:42 10/24/2017
Match information: any
Instruction information:
 Write actions:
  Drop

Flow entry 1 information:
 cookie: 0x0, priority: 1, hard time: 0, idle time: 0, flags: none,
 byte count: --, packet count: --
 Create time: 09:39:42 10/24/2017, Last modified time: 09:39:42 10/24/2017
Match information:
 Ethernet destination MAC address: 0000-0000-0001
 Ethernet destination MAC address mask: ffff-ffff-ffff
 VLAN ID: 100, mask: 0xfff
Instruction information:
 Write actions:
  Output interface: GE1/0/4
 Write metadata/mask: 0x0000000000000001/0xffffffffffffffff
 Goto table: 1
```

```
Table 1 information:
 Table type: Extensibility, flow entry count: 2, total flow entry count: 2

MissRule (default) flow entry information:
 cookie: 0x0, priority: 0, hard time: 0, idle time: 0, flags: none,
 byte count: 300, packet count: 60
 Create time: 09:39:42 10/24/2017, Last modified time: 09:39:42 10/24/2017
Match information: any
Instruction information:
 Write actions:
  Drop

Flow entry 1 information: (Not effective)
 cookie: 0x0, priority: 0, hard time: 0, idle time: 0, flags: flow_send_rem
 |check_overlap, byte count: 8, packet count: 1
 Create time: 09:39:42 10/24/2017, Last modified time: 09:39:42 10/24/2017
Match information:
 Input interface: GE1/0/3
 Ethernet source MAC address: 0000-0000-0001
 Ethernet source MAC address mask: ffff-ffff-ffff
Instruction information:
 Set meter: 100
 Apply actions:
  Output interface: GE1/0/4
 Write actions:
  Output interface: Controller, send length: 128 bytes
```

Table 3 Command output

Field	Description
Table information	Information about the flow table.
Table type	Type of the flow table: **MAC-IP** or **Extensibility**.
flow entry count	Number of flow entries deployed by the controller.
total flow entry count	Total number of flow entries in the table.
Flow entry information	Information about the flow entry. If the flow entry does not take effect, this field displays **Not effective**.
cookie	Cookie ID of the flow entry.
priority	Priority of the flow entry. The larger the value, the higher the priority.
hard time	Hard timeout of the flow entry, in seconds. The flow entry is removed when the timer times out, whether or not the flow entry matches any data stream. If the flow entry has no hard timeout, the field displays **0**.
idle time	Idle timeout of the flow entry, in seconds. The flow entry is removed if the flow entry does not match any data stream during the idle time. If the flow entry has no idle timeout, the field displays **0**.

Field	Description
flags	Flags that the flow entry includes: • **flow_send_rem**—Sends a flow removed message when the flow entry is removed or expires. • **check_overlap**—Checks for overlapping flow entries. • **reset_counts**—Resets flow table counters. • **no_pkt_counts**—Does not count packets. • **no_byte_counts**—Does not count bytes. If the flow entry does not include any flags, this field displays **none**.
byte count	Number of bytes that have matched the flow entry.
packet count	Number of packets that have matched the flow entry.
Create time	Time when the flow entry was created.
Last modified time	Time when the flow entry was modified for the last time.
Match information	Contents of the match field of the flow entry (see Table 4).
Instruction information	Contents of the instruction set of the flow entry: • **Set meter**—Sends the matched packet to a specific meter. • **Goto table**—Sends the matched packet to the next flow table for processing. • **Clear actions**—Immediately clears all actions in the action set. • **Apply actions**—Immediately applies specified actions in the action set. • **Write actions**—Writes specified actions into the current action set. For more information about actions, see Table 5.

Table 4 Match field types (supported fields vary by device model)

Field	Mask field	Description
Input interface	N/A	Ingress port (see Table 6).
Physical input interface	N/A	Ingress physical port.
Metadata	Metadata mask	Metadata and mask.
Ethernet destination MAC address	Ethernet destination MAC address mask	Ethernet destination MAC address and mask.
Ethernet source MAC address	Ethernet source MAC address mask	Ethernet source MAC address and mask.
Ethernet type	N/A	Ethernet type of the OpenFlow packet payload.
VLAN ID	Mask	VLAN ID and mask.
VLAN PCP	N/A	VLAN priority.
IP DSCP	N/A	Differentiated Services Code Point (DSCP) value.
IP ECN	N/A	Explicit Congestion Notification (ECN) value in the IP header.
IP protocol	N/A	IPv4 or IPv6 protocol number.
IPv4 source address	Mask	IPv4 source address and mask.
IPv4 destination address	Mask	IPv4 destination address and mask.
TCP source port	Mask	TCP source port and mask.

Field	Mask field	Description
TCP destination port	Mask	TCP destination port and mask.
UDP source port	Mask	UDP source port and mask.
UDP destination port	Mask	UDP destination port and mask.
ICMPv4 type	N/A	ICMPv4 type.
ICMPv4 code	N/A	ICMPv4 code.
ARP source IPv4 address	Mask	Sender IPv4 address and mask in the ARP payload.
ARP source MAC address	ARP source MAC address mask	Sender MAC address and mask in the ARP payload.
IPv6 source address	IPv6 source address mask	Source IPv6 address and mask.
IPv6 destination address	IPv6 destination address mask	Destination IPv6 address and mask.
IPv6 flow label	Mask	IPv6 flow label and mask.
ICMPv6 type	N/A	ICMPv6 type.
ICMPv6 code	N/A	ICMPv6 code.
Output interface	N/A	Output port.

Table 5 Actions

Field	Description
Drop	Drops the matched packet. This action is not defined in the OpenFlow specifications.
Output interface	Sends the packet through a specific port. For more information about ports, see Table 6.
Group	Specifies a group table to process the packet.
Set queue	Maps the flow entry to a queue specified by its ID.
Set field	Modifies a field of the packet.
Decrement IP TTL	Decreases the IP TTL by 1.

Table 6 Ports

Port name	Ingress port	Output port	Description
In port	Not supported.	Supported.	Forwarding the packet out of the ingress port.
Normal	Not supported.	Supported.	Processing the packet by using the normal forwarding process.
Flood	Not supported.	Supported.	Flooding the packet.
All	Not supported.	Supported.	Forwarding the packet out of all ports.
Controller	Supported.	Supported.	Sending the packet to the controller.
Local	Supported.	Supported.	Sending the packet to the local CPU.
Any	Not supported.	Not supported.	Special value used in some OpenFlow commands when you do not specify a port.

Port name	Ingress port	Output port	Description
port name	Supported.	Supported.	Valid physical or logical port on the switch.

display openflow group

Use **display openflow group** to display group information for an OpenFlow instance.

Syntax

display openflow instance *instance-id* **group** [*group-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

instance-id: Specifies an OpenFlow instance by its ID in the range of 1 to 4094.

group-id: Specifies a group by its ID in the range of 0 to 4294967040. If you do not specify a group ID, this command displays information about all group entries for an OpenFlow instance.

Examples

Display group information for OpenFlow instance 100.

```
<Sysname> display openflow instance 100 group
Instance 100 group table information:
 Group count: 2

Group entry 103:
 Type: All, byte count: 55116, packet count: 401
 Bucket 1 information:
  Action count 1, watch port: any, watch group: any
  Byte count 55116, packet count 401
  Output interface: BAGG100
 Bucket 2 information:
 Action count 1, watch port: any, watch group: any
  Byte count 0, packet count 0
  Output interface: Controller, send length: 128 bytes
 Referenced information:
  Count: 3
  Flow table 0
  Flow entry: 1, 2, 3

Group entry 104:
 Some buckets are invalid.
 Type: All, byte count: 0, packet count: 0
 Bucket 1 information:
  Action count 2, watch port: any, watch group: any
  Byte count 0, packet count 0
```

```
  Set field:
   Ethernet destination MAC address: 0000-0000-0013
   Ethernet source MAC address: 0000-0000-0012
   IPv4 destination address: 100.0.0.21
   UDP destination port: 1001
  Output interface: Controller, send length: 128 bytes
 Referenced information:
  Count: 0
```

Table 7 Command output

Field	Description
Group count	Total number of group entries included in the OpenFlow instance.
Some buckets are invalid.	Some buckets of the group entry are invalid because the hardware resources are insufficient or the device fails.
Type	Type of the group entry. The value of **All** indicates that the device executes all buckets in the group. This group is used for multicast or broadcast forwarding.
Bucket	Buckets included in the group table.
Action count	Number of actions included in the bucket.
Byte count	Number of bytes processed by a group or by a bucket. If the statistics cannot be collected, this field displays two hyphens (**--**).
packet count	Number of packets processed by a group or by a bucket. If the statistics cannot be collected, this field displays two hyphens (**--**).
watch port	Port whose state affects whether this bucket is live.
watch group	Group whose state affects whether this bucket is live.
Set field	Fields to be modified for packets, for example, the destination/source MAC address, destination IPv4 address, and destination UDP port number.
Output interface	OpenFlow port to which packets are forwarded.
Referenced information	Information about the group entry used by flow entries.
Count	Total number of flow entries that use the group entry.
Flow table	Flow table to which the flow entries that use the group entry belong.
Flow entry	Flow entries that use the group entry.

display openflow instance

Use **display openflow instance** to display detailed information about an OpenFlow instance.

Syntax

display openflow instance [*instance-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

instance-id: Specifies an OpenFlow instance by its ID in the range of 1 to 4094. If you do not specify an instance ID, this command displays detailed information about all OpenFlow instances.

Examples

Display detailed information about all OpenFlow instances.

```
<Sysname> display openflow instance
Instance 100 information:

Configuration information:
 Description   : test-desc
 Active status : Active
 Inactive configuration:
  None
 Active configuration:
  Classification: VLAN, loosen mode, total VLANs(1)
   2
  In-band management VLAN, total VLANs(0)
   Empty VLAN
  Connect mode: Multiple
  MAC address learning: Disabled
  TCP DSCP value: 10
  Flow table:
   Table ID(type): 0(MAC-IP), count: 0
  Flow-entry max-limit: 65535
  Datapath ID: 0x0000001234567891
  Default table-miss: Drop
  Forbidden port: None
  Qinq Network: Disabled
  TCP connection backup: Enabled
Port information:
 GigabitEthernet1/0/3
Active channel information:
 Controller 1 IP address: 192.168.49.49  port: 6633
 Controller 2 IP address: 192.168.43.49  port: 6633
…
```

Table 8 Command output

Field	Description
Configuration information	Information about the configuration.
Description	Description of the OpenFlow instance.
Active status	OpenFlow instance status: **Active** or **Inactive**.
Inactive configuration	Inactive configuration for the OpenFlow instance.
Active configuration	Active configuration for the OpenFlow instance.
Classification: VLAN, total VLANs	VLANs that are associated with the OpenFlow instance and the total number of these VLANs.

Field	Description
loose mode	The loose mode is used.
In-band management VLAN, total VLANs	Inband management VLANs and the total number of them.
Connect mode	Connection mode of the controller: • **Single**—The OpenFlow instance connects to only one controller at a time. • **Multiple**—The OpenFlow instance can simultaneously connect to multiple controllers.
MAC address learning	Whether MAC address learning is disabled: **Enabled** or **Disabled**.
TCP DSCP value	DSCP value for OpenFlow packets.
Flow table	Flow table information for the OpenFlow instance.
Table ID(type)	Type of the flow table: **MAC-IP** or **Extensibility**.
count	Total number of flow entries included in the current flow table.
Flow-entry max-limit	Maximum number of flow entries allowed in the extensibility flow table.
Datapath ID	Datapath ID of the OpenFlow instance.
Default table-miss	Default action of the table-miss flow entry: **Permit** or **Drop**.
Forbidden port	Type of interfaces that are forbidden to be reported to the controller: **VLAN interface**.
TCP connection backup	Whether OpenFlow connection backup is enabled: • **Disabled**. • **Enabled**.
Port information	Ports that have been added to the OpenFlow instance.
Active channel information	Information about active channels.
IP address	IP address of the controller configured for the OpenFlow instance.
Port	TCP port number that is used to connect to the controller.
Failopen mode	Connection interruption mode for the OpenFlow instance: • **Standalone**. • **Smart**. • **Secure**.

display openflow meter

Use **display openflow meter** to display meter information for an OpenFlow instance.

Syntax

display openflow instance *instance-id* **meter** [*meter-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

instance-id: Specifies an OpenFlow instance by its ID in the range of 1 to 4094.

meter-id: Specifies a meter by its ID in the range of 1 to 4294901760. If you do not specify a meter ID, this command displays information about all meter entries for an OpenFlow instance.

Examples

Display meter information for OpenFlow instance 100.

```
<Sysname> display openflow instance 100 meter
Meter flags: KBPS  -- Rate value in kb/s, PKTPS -- Rate value in packet/sec
             BURST -- Do burst size,      STATS -- Collect statistics

Instance 100 meter table information:
 meter entry count: 2

Meter entry 100 information:
 Meter flags: KBPS
 Band 1 information
 Type: drop, rate: 1024, burst size: 65536
 Byte count: 0, packet count: 0
 Referenced information:
  Count: 3
  Flow table: 0
  Flow entry: 1, 2, 3

Meter entry 200 information:
 Meter flags: KBPS
 Band 1 information
 Type: drop, rate: 10240, burst size: 655360
 Byte count: 0, packet count: 0
 Referenced information:
  Count: 0
```

Table 9 Command output

Field	Description
Group entry count	Total number of meter entries that the OpenFlow instance has.
Meter flags	Flags configured for the meter: • **KBPS**—The rate value is in kbps. • **PKTPS**—The rate value is in pps. • **BURST**—The burst size field in the band is used and the length of the packet or byte burst is determined by the burst size. • **STATS**—Meter statistics are collected.
Band	Bands contained in the meter.
Type	Type of the band: • **drop**—Discard the packet. • **dscp_remark**—Modify the drop precedence of the DSCP field in the IP header of the packet.

Field	Description
Rate	Rate value above which the corresponding band applies to packets.
Burst size	Length of the packet or byte burst to consider for applying the meter.
Byte count	Number of bytes processed by a band. If the statistics cannot be collected, this field displays two hyphens (**--**).
packet count	Number of packets processed by a band. If the statistics cannot be collected, this field displays two hyphens (**--**).
Referenced information	Information about the meter entry used by flow entries.
Count	Total number of flow entries that use the meter entry.
Flow table	Flow table to which the flow entries that use the meter entry belong.
Flow entry	Flow entries that use the meter entry.

display openflow summary

Use **`display openflow summary`** to display brief OpenFlow instance information.

Syntax

`display openflow instance summary`

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display brief OpenFlow instance information.

```
<Sysname> display openflow summary
Fail-open mode: Se - Secure mode, Sa - Standalone mode, Sm - Smart mode

ID    Status    Datapath-ID         Channel    Table-num  Port-num  Reactivate
1     Active    0x0000000100001221  Connected  2          8         N
10    Inactive  -                   -          -          -         -
4094  Active    0x00000ffe00001221  Failed(Sa) 2          0         N
```

Table 10 Command output

Field	Description
ID	OpenFlow instance ID.
Status	Activation status of the OpenFlow instance: • **Active**—The OpenFlow instance has been activated. • **Inactive**—The OpenFlow instance has not been activated.
Datapath-ID	Datapath ID of the OpenFlow instance. If the OpenFlow instance is not activated, this field displays a hyphen (**-**).

Field	Description
Channel	Status of the OpenFlow channel to the controller: • **Connected**—An OpenFlow channel has been established. • **Failed(Se)**—The OpenFlow channel is disconnected from the controller, and the OpenFlow instance uses the **secure** connection interruption mode. • **Failed(Sm)**—The OpenFlow channel is disconnected from the controller, and the OpenFlow instance uses the **smart** connection interruption mode. • **Failed(Sa)**—The OpenFlow channel is disconnected from the controller, and the OpenFlow instance uses the **standalone** connection interruption mode. If the OpenFlow instance is not activated, this field displays a hyphen (**-**).
Table num	Number of flow tables that the OpenFlow instance has. If the OpenFlow instance is not activated, this field displays a hyphen (**-**).
Port num	Number of ports that belong to the OpenFlow instance. If the OpenFlow instance is not activated, this field displays a hyphen (**-**).
Reactivate	Whether the OpenFlow instance is required to be reactivated. **N** indicates the configuration is unchanged and the OpenFlow instance is not required to be reactivated. If the OpenFlow instance is not activated, this field displays a hyphen (**-**).

fail-open mode

Use **fail-open mode** to set the connection interruption mode for an OpenFlow switch.

Use **undo fail-open mode** to restore the default.

Syntax

fail-open mode { **secure** | **smart** | **standalone** }

undo fail-open mode

Default

The connection interruption mode is **secure**.

Views

OpenFlow instance view

Predefined user roles

network-admin

Parameters

secure: Configures the OpenFlow switch to use flow tables for traffic forwarding after it is disconnected from all controllers. The OpenFlow switch does not remove unexpired flow entries.

smart: Configures the OpenFlow switch to use flow tables for traffic forwarding after it is disconnected from all controllers. If the output action in a matching flow entry is to forward traffic to a controller, the traffic is forwarded in normal process.

standalone: Configures the OpenFlow switch to use the normal forwarding process after it is disconnected from all controllers.

Examples

Set the connection interruption mode to **standalone** for OpenFlow instance 1.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] fail-open mode standalone
```

flow-entry max-limit

Use **flow-entry max-limit** to set the maximum number of entries for an extensibility flow table on an OpenFlow switch.

Use **undo flow-entry max-limit** to restore the default.

Syntax

flow-entry max-limit *limit-value*

undo flow-entry max-limit

Default

An extensibility flow table can have a maximum of 65535 flow entries.

Views

OpenFlow instance view

Predefined user roles

network-admin

Parameters

limit-value: Specifies the maximum number of flow entries for an extensibility flow table. The value range for this argument is 1 to 65535.

Usage guidelines

If the number of extensibility flow table entries deployed from a controller to an OpenFlow switch exceeds the maximum, the switch returns a failure message to the controller.

Examples

Configure OpenFlow instance 1 to have a maximum of 256 entries in each extensibility flow table.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] flow-entry max-limit 256
```

flow-log disable

Use **flow-log disable** to disable logging for successful flow table modifications.

Use **undo flow-log disable** to restore the default.

Syntax

flow-log disable

undo flow-log disable

Default

Logging for successful flow table modifications is enabled.

Views

OpenFlow instance view

Predefined user roles

network-admin

Examples

Disable logging for successful flow table modifications for OpenFlow instance 1.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] flow-log disable
```

flow-table

Use **flow-table** to configure the flow table type and the flow table ID for an OpenFlow instance.

Use **undo flow-table** to restore the default.

Syntax

flow-table { **extensibility** *extensibility-table-id* | **mac-ip** *mac-ip-table-id* }*

undo flow-table

Default

An OpenFlow instance has an extensibility flow table with ID 0.

Views

OpenFlow instance view

Predefined user roles

network-admin

Parameters

extensibility *extensibility-table-id*: Specifies an extensibility flow table by its ID in the range of 0 to 254.

mac-ip *mac-ip-table-id*: Specifies a MAC-IP flow table by its ID in the range of 0 to 254.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

The ID you enter for an extensibility flow table must be larger than the ID for an MAC-IP flow table.

Examples

Create a MAC-IP flow table with ID 0 and an extensibility flow table with ID 1 for OpenFlow instance 1.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] flow-table mac-ip 0 extensibility 1
```

forbidden packet-in arp controller

Use **forbidden packet-in arp controller** to configure controllers to which ARP packets are forbidden to be reported.

Use **undo forbidden packet-in arp controller** to restore the default.

Syntax

forbidden packet-in arp controller *controller-id-list*

undo forbidden packet-in arp controller [*controller-id-list*]

Default

No controllers to which ARP packets are forbidden to be reported are configured.

Views

OpenFlow instance view

Predefined user roles

network-admin

Parameters

controller-id-list: Specifies a space-separated list of a maximum of 10 controller items. Each item specifies a controller ID or a range of controller IDs in the form of *controller-id1* **to** *controller-id2*. The value range for controller IDs is 0 to 63. The value for the *controller-id2* argument must be equal to or greater than the value for the *controller-id1* argument. If you do not specify the *controller-id-list* argument, the **undo** form of this command restores all configuration of this feature to the default.

Examples

Forbid the device not to report ARP packets to controller 0.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] forbidden packet-in arp controller 0
```

forbidden port

Use **forbidden port** to forbid an OpenFlow instance from reporting ports of the specified types to controllers.

Use **undo forbidden port** to restore the default.

Syntax

forbidden port { **l3-physical-interface** | **vlan-interface** | **vsi-interface** } *

undo forbidden port

Default

No port types are prevented from being reported to the controllers. All ports that belong to an OpenFlow instance are reported to the controllers.

Views

OpenFlow instance view

Predefined user roles

network-admin

Parameters

l3-physical-interface: Specifies Layer 3 Ethernet interfaces and Layer 3 aggregate interfaces that belong to an OpenFlow instance. This field is not supported in the current software version.

vlan-interface: Specifies VLAN interfaces that belong to an OpenFlow instance.

vsi-interface: Specifies virtual switch instance (VSI) interfaces that belong to an OpenFlow instance. This field is not supported in the current software version.

Examples

Forbid OpenFlow instance 1 from reporting VLAN interfaces that belong to the OpenFlow instance to controllers.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] forbidden port vlan-interface
```

in-band management vlan

Use **in-band management vlan** to configure inband management VLANs for an OpenFlow instance.

Use **undo in-band management vlan** to restore the default.

Syntax

in-band management vlan *vlan-id-list*

undo in-band management vlan

Default

No inband management VLANs are configured for an OpenFlow instance.

Views

OpenFlow instance view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* **to** *end-vlan-id*. The VLAN ID is in the range of 1 to 4094.

Usage guidelines

Traffic in inband management VLANs is forwarded in the normal forwarding process for an OpenFlow instance to establish secure connections to controllers.

Examples

Configure VLAN 10 as the inband management VLAN for OpenFlow instance 1.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] in-band management vlan 10
```

listening port

Use **listening port** to configure an OpenFlow instance to act as an SSL server to listen to controllers.

Use **undo listening port** to restore the default.

Syntax

listening port *port-number* **ssl** *ssl-policy-name*

undo listening port

Default

An OpenFlow instance is not configured to acts as an SSL server to listen to controllers.

Views

OpenFlow instance view

Predefined user roles

network-admin

Parameters

port-number: Specifies the SSL server port number in the range of 1 to 65535.

ssl *ssl-policy-name*: Specifies the SSL server policy name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

Typically, an OpenFlow instance actively connects to the controller and acts as a TCP/SSL client. After the SSL server is enabled for an OpenFlow instance, the controller acts as the SSL client and actively connects to the OpenFlow instance. For more information about SSL, see *Security Configuration Guide*.

To re-configure the SSL server, first execute the **undo** form of the command to delete the existing SSL server configuration.

Examples

Configure OpenFlow instance 1 to act as an SSL server with port number 20000 and SSL server policy name **ssl_name**.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] listening port 20000 ssl ssl_name
```

loop-protection enable

Use **loop-protection enable** to enable loop guard for an OpenFlow instance.

Use **undo loop-protection enable** to restore the default.

Syntax

loop-protection enable

undo loop-protection enable

Default

Loop guard is disabled for an OpenFlow instance.

Views

OpenFlow instance view

Predefined user roles

network-admin

Usage guidelines

After an OpenFlow instance is deactivated, loops might occur in VLANs associated with the OpenFlow instance. To avoid loops, you can enable loop guard for the OpenFlow instance. This feature enables the deactivated OpenFlow instance to create a flow entry for dropping all traffic in theses VLANs.

Examples

Enable loop guard for OpenFlow instance 1.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] loop-protection enable
```

mac-ip dynamic-mac aware

Use **mac-ip dynamic-mac aware** to configure an OpenFlow instance to support matching the dynamic MAC addresses in the query and deletion flow entry instructions sent from controllers.

Use **undo mac-ip dynamic-mac aware** to restore the default.

Syntax

mac-ip dynamic-mac aware

undo mac-ip dynamic-mac aware

Default

An OpenFlow instance ignores the dynamic MAC addresses in the query and deletion flow entry instructions sent from controllers.

Views

OpenFlow instance view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only on MAC-IP flow tables.

Examples

Configure OpenFlow instance 1 to support matching the dynamic MAC addresses in the query and deletion flow entry instructions sent from controllers.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] mac-ip dynamic-mac aware
```

mac-learning forbidden

Use **mac-learning forbidden** to configure OpenFlow to forbid MAC address learning in VLANs associated with an OpenFlow instance.

Use **undo mac-learning forbidden** to restore the default.

Syntax

mac-learning forbidden

undo mac-learning forbidden

Default

MAC address learning is allowed for VLANs associated with an OpenFlow instance.

Views

OpenFlow instance view

Predefined user roles

network-admin

Examples

Forbid MAC address learning in VLANs associated with OpenFlow instance 1.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] mac-learning forbidden
```

openflow instance

Use **openflow instance** to create an OpenFlow instance and enter its view, or enter the view of an existing OpenFlow instance.

Use **undo openflow instance** to remove an OpenFlow instance.

Syntax

openflow instance *instance-id*

undo openflow instance *instance-id*

Default

No OpenFlow instances exist.

Views

System view

Predefined user roles

network-admin

Parameters

instance-id: Specifies an OpenFlow instance by its ID in the range of 1 to 4094.

Examples

Create OpenFlow instance 1 and enter OpenFlow instance view.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1]
```

openflow shutdown

Use **openflow shutdown** to shut down an interface by OpenFlow.

Use **undo openflow shutdown** to restore the default.

Syntax

openflow shutdown

undo openflow shutdown

Default

An interface is not shut down by OpenFlow.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

After an interface is shut down by OpenFlow, the **Current state** field displays **OFP DOWN** in the **display interface** command output.

To bring up an interface shut down by OpenFlow, use either of the following methods:

- Use the **undo openflow shutdown** command on the interface.
- Use the controller to send port modification messages to the interface.

Examples

Shut down GigabitEthernet 1/0/1 by OpenFlow.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] openflow shutdown
```

permit-port-type member-port

Use **permit-port-type member-port** to allow link aggregation member ports to be in the deployed flow tables.

Use **undo permit-port-type** to restore the default.

Syntax

permit-port-type member-port

undo permit-port-type

Default

Link aggregation member ports cannot be in the deployed flow tables.

Views

OpenFlow instance view

Predefined user roles

network-admin

Examples

Configure OpenFlow instance 1 to allow link aggregation member ports to be in the deployed flow tables.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] permit-port-type member-port
```

precedence dynamic arp

Use **precedence dynamic arp** to allow dynamic ARP entries to overwrite OpenFlow ARP entries.

Use **undo precedence dynamic** to restore the default.

Syntax

precedence dynamic arp

undo precedence dynamic arp

Default

An OpenFlow instance does not allow dynamic ARP entries to overwrite OpenFlow ARP entries.

Views

OpenFlow instance view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only on the MAC-IP flow table of an OpenFlow instance.

Examples

Configure OpenFlow instance 1 to allow dynamic ARP entries to overwrite OpenFlow ARP entries.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] precedence dynamic arp
```

refresh ip-flow

Use **refresh ip-flow** to refresh all Layer 3 flow entries in the MAC-IP flow tables for an OpenFlow instance.

Syntax

refresh ip-flow

Views

OpenFlow instance view

Predefined user roles

network-admin

Usage guidelines

Layer 3 flow entries in the MAC-IP flow tables might be overwritten. In such cases, you can use this command to obtain all Layer 3 flow entries in the MAC-IP flow tables from the controller again.

Examples

Refresh all Layer 3 flow entries in the MAC-IP flow tables for OpenFlow instance 1.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] refresh ip-flow
```

reset openflow instance statistics

Use **reset openflow instance statistics** to clear statistics on packets that a controller sends and receives for an OpenFlow instance.

Syntax

reset openflow instance *instance-id* { **controller** [*controller-id*] | **listened** } **statistics**

Views

User view

Predefined user roles

network-admin

Parameters

instance-id: Specifies an OpenFlow instance by its ID in the range of 1 to 4094.

controller-id: Specifies a controller by its ID in the range of 0 to 63. If you do not specify a controller ID, this command clears statistics on packets that all controllers send and receive for an OpenFlow instance.

listened: Specifies the client that connects to the server enabled for the OpenFlow instance.

Examples

Clear statistics on packets that all controllers send and receive for OpenFlow instance 1.

```
<Sysname> reset openflow instance 1 controller statistics
```

tcp dscp

Use **tcp dscp** to set a DSCP value for OpenFlow packets.

Use **undo tcp dscp** to restore the default.

Syntax

tcp dscp *dscp-value*

undo tcp dscp

Default

The DSCP value for OpenFlow packets is not set.

Views

OpenFlow instance view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies a DSCP value for OpenFlow packets, in the range of 0 to 63.

Examples

Set the DSCP value to 63 for OpenFlow packets.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] tcp dscp 63
```

tcp-connection backup

Use **tcp-connection backup** to enable OpenFlow connection backup.

Use **undo tcp-connection backup** to disable OpenFlow connection backup.

Syntax

tcp-connection backup

undo tcp-connection backup

Default

OpenFlow connection backup is enabled.

Views

OpenFlow instance view

Predefined user roles

network-admin

Usage guidelines

This command enables an OpenFlow instance to back up OpenFlow connections established over TCP. This prevents connection interruption when an active/standby switchover occurs.

This feature is available only on an IRF fabric with two member devices.

Examples

Disable OpenFlow connection backup for OpenFlow instance 1.

```
<Sysname> system-view
[Sysname] openflow instance 1
[Sysname-of-inst-1] undo tcp-connection backup
```